aws

Guia do Desenvolvedor

# Amazon Route 53 Application Recovery Controller

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon Route 53 Application Recovery Controller: Guia do Desenvolvedor

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

# Table of Contents

# O que é o Controlador de recuperação de aplicações do Amazon Route 53?

O Controlador de Recuperação de Aplicações do Amazon Route 53 ajuda você a se preparar e realizar operações de recuperação mais rápidas para aplicações em execução na AWS. O Route 53 ARC fornece quatro recursos: verificação de prontidão, controle de roteamento, mudança de zona e mudança automática de zona. Com o Route 53 ARC, você pode saber se seus aplicativos e recursos estão preparados para recuperação e mitigar rapidamente as deficiências de uma zona de disponibilidade múltipla ou de uma aplicação multirregional.

A infraestrutura de nuvem AWS global fornece tolerância a falhas e resiliência, com cada uma Região da AWS composta por várias zonas de disponibilidade totalmente isoladas. O Route 53 ARC funciona dentro dessa AWS estrutura para ajudar seus aplicativos a serem resilientes.

Recuperação multi-AZ

As mudanças de zona permitem que você se recupere rapidamente das deficiências da zona de disponibilidade, transferindo temporariamente o tráfego de um recurso para fora de uma zona de disponibilidade. Iniciar uma mudança de zona ajuda seu aplicativo a se recuperar rapidamente, por exemplo, da implantação de código incorreto de um desenvolvedor ou de uma falha de AWS infraestrutura em uma única zona de disponibilidade, reduzindo o impacto e o tempo perdidos com um problema em uma zona.

Você pode iniciar uma mudança de zona para qualquer recurso gerenciado em sua conta em uma região. Os AWS recursos suportados são registrados automaticamente no Route 53 ARC. Os recursos registrados para mudanças de zona no Route 53 ARC são recursos gerenciados nele.

As mudanças de zona são temporárias. Você deve especificar uma expiração de até três dias ao iniciar uma mudança de zona. Se você ainda quiser manter o tráfego longe de uma zona de disponibilidade, pode atualizar a mudança de zona e definir uma nova expiração.

O deslocamento automático zonal é um recurso do Route 53 ARC que permite que você AWS transfira o tráfego de uma zona de disponibilidade para um recurso, em seu nome. AWS inicia um deslocamento automático quando a telemetria interna indica que há uma deficiência na zona de disponibilidade que pode afetar potencialmente os clientes. A telemetria interna incorpora métricas de várias fontes, incluindo a AWS rede e os serviços Amazon EC2 e Elastic Load Balancing.

Recuperação multirregional

Os controles de roteamento permitem que você reequilibre o tráfego entre réplicas de aplicativos durante falhas, para garantir que seu aplicativo esteja disponível. As regras de segurança ajudam a protegê-lo de resultados não intencionais, impondo grades de proteção que você definirá. Usando essas regras, você pode garantir, por exemplo, que apenas um de seus endpoints, ativo ou em espera, esteja ativado e em serviço por vez.

Para recuperação em várias regiões, o Route 53 ARC pode ajudá-lo a coordenar centralmente os failovers em várias regiões. AWS Controles de roteamento extremamente confiáveis permitem que você recupere aplicativos redirecionando o tráfego, por exemplo, entre regiões. Para fazer isso, você particiona seus aplicativos em unidades redundantes de contenção de falhas ou réplicas. O limite de cada réplica pode ser uma região ou uma zona de disponibilidade, ou até mesmo uma unidade menor.

As verificações de prontidão monitoram continuamente as cotas de AWS recursos, a capacidade e as políticas de roteamento de rede e podem notificá-lo sobre alterações que afetariam sua capacidade de fazer o failover para uma réplica e se recuperar. As verificações contínuas de prontidão ajudam a garantir que, de forma regular, seus aplicativos multirregionais sejam escalados e configurados para lidar com o tráfego de failover.

Tópicos



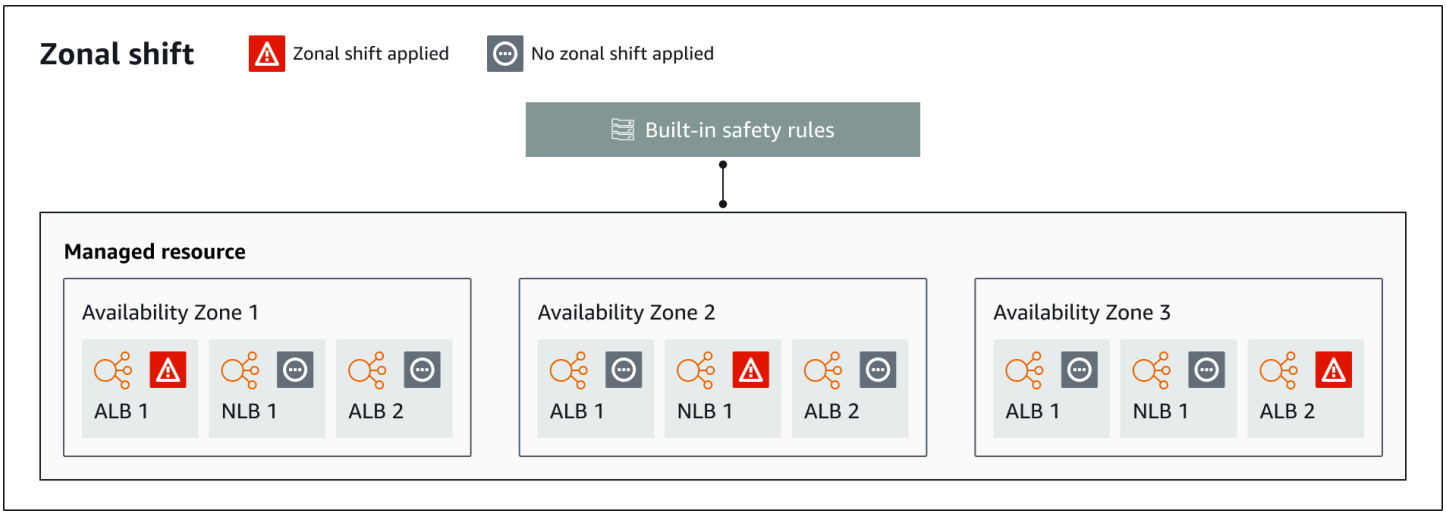
# Componentes do Controlador de recuperação de aplicações do Amazon Route 53

Esta seção define os componentes incluídos nos recursos de mudança de zona, mudança automática de zona, verificação de prontidão e controle de roteamento do Controlador de Recuperação de Aplicações do Amazon Route 53.

- 
- 
- 
- 

## Componentes da mudança de zona

O diagrama a seguir ilustra um exemplo de uma mudança de zona afastando o tráfego de uma zona de disponibilidade em uma região. AWS As regras de segurança incorporadas ao Route 53 ARC evitam que você inicie outra mudança de zona para um recurso quando ele já tem uma mudança de zona ativa.




Veja a seguir os componentes dos recursos de mudança de zona no Route 53 ARC.

Mudança de zona

Você inicia uma mudança de zona para um recurso gerenciado em sua AWS conta para afastar temporariamente o tráfego de uma zona de disponibilidade em uma AWS região. Os AWS recursos compatíveis são registrados automaticamente no Route 53 ARC e, em seguida, são recursos gerenciados para mudanças de zona em sua conta. Atualmente, você pode iniciar uma mudança de zona somente para Network Load Balancers e Application Load Balancers que não tenham o balanceador de carga entre zonas configurado.

Iniciar uma mudança de zona ajuda seu aplicativo a se recuperar rapidamente, por exemplo, da implantação de código incorreto de um desenvolvedor ou de uma falha de AWS infraestrutura em

uma única zona de disponibilidade, reduzindo o impacto e o tempo perdidos com um problema em uma zona.

Regras de segurança integradas

As regras de segurança integradas ao Route 53 ARC evitam que mais de uma mudança de tráfego entre em vigor ao mesmo tempo para um recurso. Ou seja, somente uma mudança de zona iniciada pelo cliente, uma mudança de zona de execução prática ou uma mudança automática para o recurso pode estar ativamente transferindo o tráfego para fora de uma zona de disponibilidade. Por exemplo, se você iniciar uma mudança de zona para um recurso enquanto ele estiver deslocado por uma mudança automática, a mudança de zona terá precedência. Para obter mais informações, consulte Mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53 e Resultados das execuções práticas.

Identificador do recurso

O identificador de um recurso a ser incluído em uma mudança de zona. O identificador do recurso é um nome do recurso da Amazon (ARN).

Você só pode incluir em uma mudança de zona os recursos em sua conta que estão em um serviço da AWS compatível com o Route 53 ARC. Os recursos nesses AWS serviços são registrados no Route 53 ARC pelo AWS serviço.

> **Note**
>
> Só é possível iniciar uma mudança de zona para Network Load Balancers e Application Load Balancers com o balanceamento de carga entre zonas desativado.

Atributos gerenciados

AWS os serviços registram recursos automaticamente com o Route 53 ARC para mudança zonal. Um recurso que foi registrado é um recurso gerenciado no Route 53 ARC.

Nome do recurso

O nome de um recurso gerenciado no Route 53 ARC.

Status (status de mudança de zona)

Um status para uma mudança de zona. O `Status` para uma mudança de zona pode ter um dos seguintes valores:

- ATIVO: a mudança de zona é iniciada e ativada.
- EXPIRADO: a mudança de zona expirou, ou seja, o tempo de expiração foi excedido.
- CANCELADO: a mudança de zona foi cancelada.

Status aplicado

Um status aplicado indica se uma mudança de tráfego está em vigor para um recurso. A mudança que tem o status `APPLIED` determina a zona de disponibilidade em que o tráfego da aplicação foi deslocado para um recurso e quando essa mudança de tráfego terminará.

Tempo de expiração

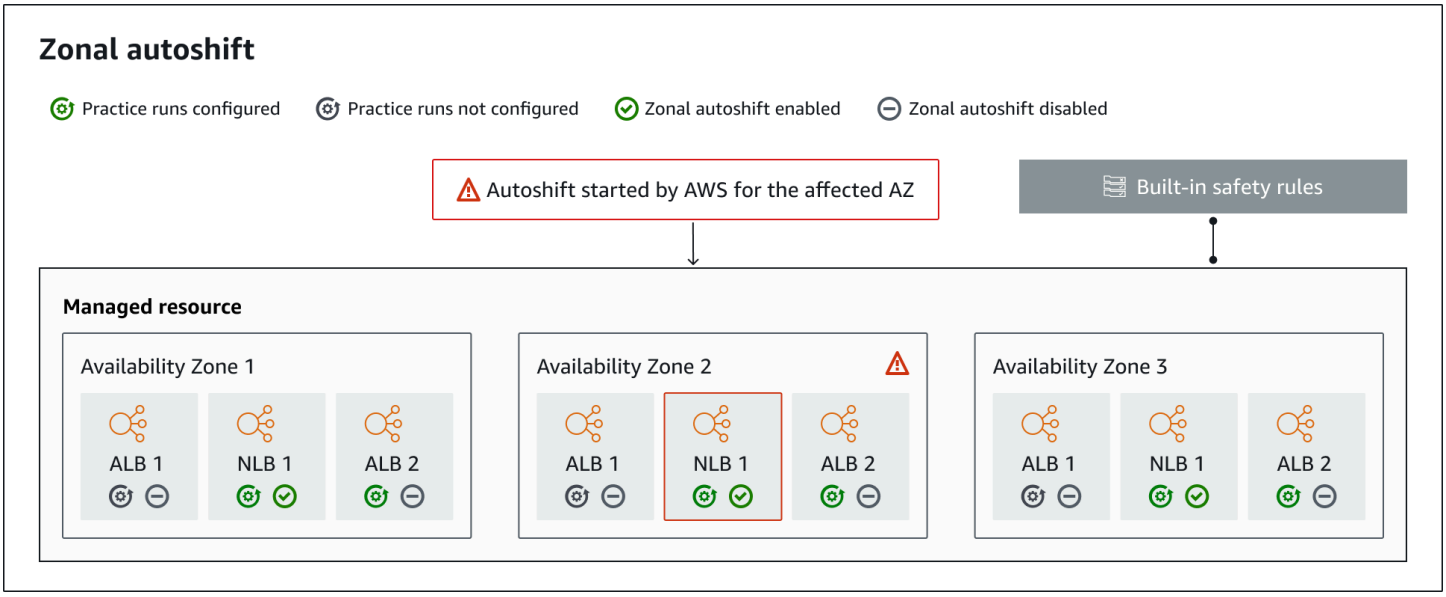
O tempo de expiração para uma mudança de zona. As mudanças de zona são temporárias. Para uma mudança de zona iniciada pelo cliente, você pode definir inicialmente que a mudança de zona fique ativa por até três dias (72 horas).

Ao iniciar uma mudança de zona, você especifica por quanto tempo deseja que ela fique ativa, o que o Route 53 ARC converte em um tempo de expiração. Você pode cancelar uma mudança de zona iniciada pelo cliente, por exemplo, se estiver com tudo pronto para restaurar o tráfego para a zona de disponibilidade. Ou você pode estender uma mudança de zona iniciada pelo cliente, atualizando-a para especificar outro período de tempo para expirar.

Você pode cancelar tanto os turnos zonais iniciados pelo cliente quanto os turnos zonais que AWS começam em uma execução prática com o deslocamento automático zonal.

## Componentes da mudança automática de zona

O diagrama a seguir ilustra um exemplo de uma mudança automática transferindo o tráfego para fora de uma zona de disponibilidade quando a telemetria interna indica que há uma deficiência na zona de disponibilidade capaz de afetar os clientes.




Veja a seguir os componentes dos recursos de mudança automática de zona no Route 53 ARC.

Mudança automática de zona

A mudança automática de zona desloca o tráfego de um recurso, sem exigir que você execute nenhuma ação. O deslocamento automático zonal é um recurso do Route 53 ARC que AWS inicia um deslocamento automático quando a telemetria interna indica que há uma deficiência na zona de disponibilidade que poderia impactar os clientes. Esteja ciente de que, em alguns casos, podem haver transferência de recursos que não estão sofrendo impacto.

Execuções práticas

Ao habilitar o deslocamento automático zonal para um recurso, você também deve configurar execuções práticas de mudança automática zonal para o recurso. AWS realiza uma mudança zonal para treinos semanais, por cerca de 30 minutos. As execuções práticas garantem que a aplicação possa ser executada normalmente com a perda de uma zona de disponibilidade. Em uma execução prática, AWS desloca o tráfego de um recurso para fora de uma zona de disponibilidade com uma mudança zonal e, em seguida, transfere o tráfego de volta quando a execução prática termina.

Configuração de execução prática

Uma configuração de execução prática define as datas e janelas bloqueadas, se houver, e os CloudWatch alarmes que você especifica para a execução prática de um recurso no deslocamento automático zonal. Você pode editar uma execução prática a qualquer momento,

para adicionar ou alterar datas ou janelas bloqueadas ou para atualizar os alarmes da execução prática.

Para habilitar a mudança automática de zona, é necessário ter uma configuração de execução prática para um recurso. Você também pode excluir uma execução prática. Para excluir uma configuração de execução prática de um recurso, a mudança automática de zona deve estar desabilitada.

Alarme de execução prática

Ao configurar execuções práticas, você especifica CloudWatch os alarmes criados em CloudWatch, com base nos requisitos de recursos e aplicativos. Os alarmes que você especifica podem impedir o início de uma execução prática ou interromper uma execução prática em andamento, caso a aplicação seja afetada adversamente pela execução prática.

Se um alarme que você especificar entrar em um estado `ALARM`, o Route 53 ARC encerrará a mudança de zona para a execução prática, de modo que o tráfego do recurso não seja mais transferido para fora da zona de disponibilidade.

Há dois tipos de alarmes que você especifica para as execuções práticas: um alarme de resultado, para monitorar a integridade do recurso e da aplicação durante a execução prática, e um alarme de bloqueio, que você pode configurar para impedir que as execuções práticas sejam iniciadas ou para interromper uma execução prática em andamento. O alarme de resultado é obrigatório, enquanto o alarme de bloqueio é opcional.

Resultado da execução prática

Para cada execução prática, o Route 53 ARC relata um resultado. Veja a seguir os possíveis resultados para uma execução prática:

- PENDENTE: a mudança de zona para a execução prática está ativa (em andamento). Ainda não há resultado a ser retornado.
- BEM-SUCEDIDA: o alarme de resultado não entrou em um estado `ALARM` durante a execução prática e ela concluiu todo o período de teste de 30 minutos.
- INTERROMPIDA: a execução prática foi encerrada por um motivo que não foi o alarme de resultado entrando em um estado `ALARM`. Uma execução prática pode ser interrompida por vários motivos. Por exemplo, uma execução prática que termina porque o alarme de bloqueio especificado para a execução prática entrou em um estado `ALARM` tem um resultado `INTERRUPTED`. Para obter mais informações sobre os motivos para um resultado `INTERRUPTED`, consulte Resultados das execuções práticas.

- FALHOU: o alarme de resultado entrou em um estado `ALARM` durante a execução prática.

Regras de segurança integradas

As regras de segurança integradas ao Route 53 ARC evitam que mais de uma mudança de tráfego entre em vigor ao mesmo tempo para um recurso. Ou seja, somente uma mudança de zona iniciada pelo cliente, uma mudança de zona de execução prática ou uma mudança automática para o recurso pode estar ativamente transferindo o tráfego para fora de uma zona de disponibilidade. Por exemplo, se você iniciar uma mudança de zona para um recurso enquanto ele estiver deslocado por uma mudança automática, a mudança de zona terá precedência. Para obter mais informações, consulte Mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53 e Resultados das execuções práticas.

Identificador do recurso

O identificador de um recurso a ser incluído em uma mudança de zona. O identificador do recurso é um nome do recurso da Amazon (ARN).

Você só pode incluir em uma mudança de zona os recursos em sua conta que estão em um serviço da AWS compatível com o Route 53 ARC. Os recursos nesses AWS serviços são registrados no Route 53 ARC pelo AWS serviço.

> **Note**
>
> Só é possível configurar uma mudança automática de zona para Network Load Balancers e Application Load Balancers com o balanceamento de carga entre zonas desativado.

Atributos gerenciados

AWS os serviços registram recursos automaticamente com o Route 53 ARC para mudança automática zonal. Um recurso que foi registrado é um recurso gerenciado no Route 53 ARC.

Nome do recurso

O nome de um recurso gerenciado no Route 53 ARC.

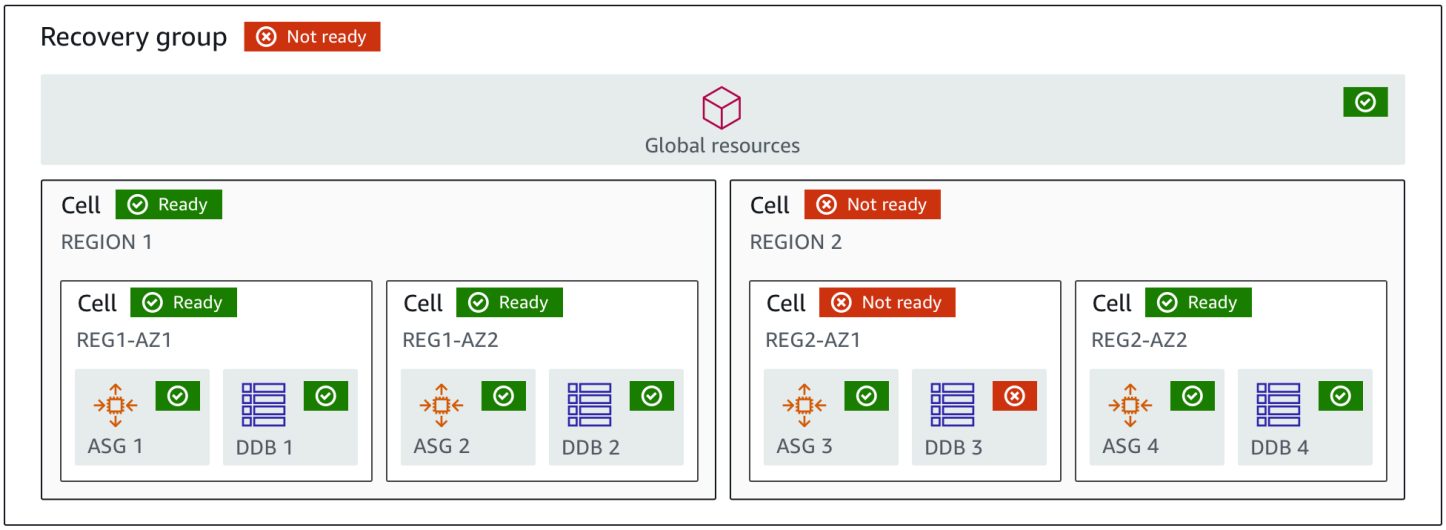
Status aplicado

Um status aplicado indica se uma mudança de tráfego está em vigor para um recurso. Quando você configura a mudança automática de zona, um recurso pode ter mais de uma transferência

de tráfego ativa, ou seja, uma mudança de zona para execução prática, uma mudança de zona iniciada pelo cliente ou uma mudança automática. No entanto, somente uma é aplicada, ou seja, somente uma está em vigor para o recurso por vez. A mudança que tem o status `APPLIED` determina a zona de disponibilidade em que o tráfego da aplicação foi deslocado para um recurso e quando essa mudança de tráfego terminará.

## Componentes da verificação de prontidão

O diagrama a seguir ilustra um exemplo de grupo de recuperação configurado para oferecer suporte ao atributo de verificação de prontidão. Os recursos neste exemplo são agrupados em células (por região da AWS ) e células aninhadas (por zonas de disponibilidade) em um grupo de recuperação. Há um status geral de prontidão para o grupo de recuperação (aplicativo), bem como status de prontidão individual para cada célula (região) e célula aninhada (zona de disponibilidade).




A seguir estão os componentes do recurso de verificação de prontidão no Route 53 ARC.

Célula

Uma célula define as réplicas ou unidades independentes de failover do seu aplicativo. Ele agrupa todos os AWS recursos necessários para que seu aplicativo seja executado de forma independente na réplica. Por exemplo, você pode ter um conjunto de recursos em uma célula primária e outro em uma célula em espera. Você determina o limite do que uma célula inclui, mas as células normalmente representam uma zona de disponibilidade ou uma região. Você pode ter várias células aninhadas em uma célula, como AZs em uma região. Cada célula aninhada representa uma unidade isolada de failover.

Grupo de recuperação

As células são coletadas em um grupo de recuperação. Um grupo de recuperação representa um aplicativo ou grupo de aplicativos que você deseja verificar se está pronto para o failover. Consiste em duas ou mais células, ou réplicas, que se combinam em termos de funcionalidade. Por exemplo, se você tiver um aplicativo da web que é replicado em us-east-1a e us-east-1b, onde us-east-1b é seu ambiente de failover, é possível representar esse aplicativo no Route 53 ARC como um grupo de recuperação com duas células: uma em us-east-1a e outra em us-east-1b. Um grupo de recuperação também pode incluir um recurso global, como uma verificação de integridade do Route 53.

Recursos e identificadores de recursos

Ao criar componentes para verificações de prontidão no Route 53 ARC, você especifica um recurso, como uma tabela do Amazon DynamoDB, um Network Load Balancer ou um recurso de destino de DNS, usando um identificador. Um identificador de recurso é o número de recurso da Amazon (ARN) ou, para um recurso de destino de DNS, o identificador que o Route 53 ARC gera ao criá-lo.

Recurso de destino DNS

Um recurso de destino de DNS é a combinação do nome de domínio do seu aplicativo e outras informações de DNS, como o AWS recurso para o qual o domínio aponta. Incluir um recurso da AWS é opcional, mas se você o fornecer, deverá ser um registro de recurso do Route 53 ou um Network Load Balancer. Ao fornecer o AWS recurso, você pode obter recomendações arquitetônicas mais detalhadas que podem ajudá-lo a melhorar a resiliência de recuperação do seu aplicativo. Você pode criar conjuntos de recursos no Route 53 ARC para recursos de destino de DNS e, em seguida, criar uma verificação de prontidão para o conjunto de recursos para obter recomendações de arquitetura para seu aplicativo. A verificação de prontidão também monitora a política de roteamento de DNS do seu aplicativo, com base nas regras de prontidão para os recursos de destino do DNS.

Conjunto de recursos

Um conjunto de recursos é um conjunto de recursos, incluindo AWS recursos ou recursos de destino de DNS, que abrangem várias células. Por exemplo, é possível ter um balanceador de carga em us-east-1a e outro em us-east-1b. Para monitorar a prontidão de recuperação dos balanceadores de carga, você pode criar um conjunto de recursos que inclua os dois balanceadores de carga e, em seguida, criar uma verificação de prontidão para o conjunto de recursos. O Route 53 ARC verificará continuamente a disponibilidade dos recursos no conjunto.

Você também pode adicionar um escopo de prontidão para associar recursos em um conjunto ao grupo de recuperação que você criar para seu aplicativo.

Regra de prontidão

As regras de prontidão são auditorias que o Route 53 ARC executa em relação a um conjunto de recursos. O Route 53 ARC tem um conjunto de regras de prontidão para cada tipo de recurso para o qual ele dá suporte. Cada regra inclui um ID e uma descrição que explicam por que o Route 53 ARC inspeciona os recursos.

Verificação de prontidão

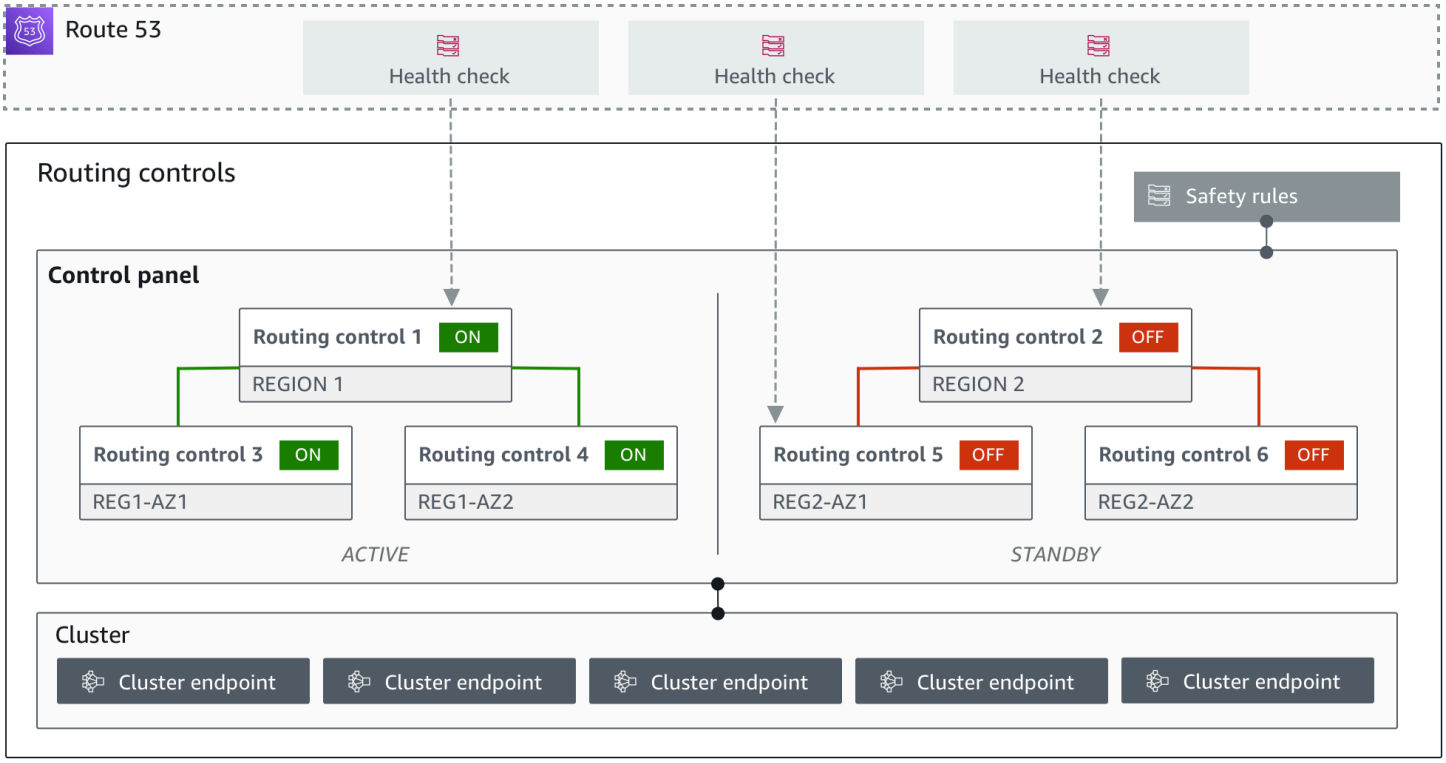
Uma verificação de prontidão monitora um conjunto de recursos no aplicativo, como um conjunto de instâncias do Amazon Aurora, que o Route 53 ARC audita por prontidão de recuperação. As verificações de prontidão podem incluir auditorias, por exemplo, configurações de capacidade, AWS cotas ou políticas de roteamento. Por exemplo, se você quiser auditar a prontidão de seus grupos do Amazon EC2 Auto Scaling em duas zonas de disponibilidade, você pode criar uma verificação de prontidão para um conjunto de recursos com dois ARNs de recursos, um para cada grupo do Auto Scaling. Em seguida, para garantir que cada grupo seja escalado igualmente, o Route 53 ARC monitora continuamente os tipos de instância e as contagens nos dois grupos.

Escopo de prontidão

Um escopo de prontidão identifica o agrupamento de recursos que uma verificação de prontidão específica abrange. O escopo de uma verificação de prontidão pode ser um grupo de recuperação (global para todo o aplicativo) ou uma célula (uma região ou zona de disponibilidade). Para um recurso global para o Route 53 ARC, defina o escopo de prontidão no nível do grupo de recuperação ou do recurso global. Por exemplo, uma verificação de integridade do Route 53 é um recurso global no Route 53 ARC porque não é específica para uma região ou zona de disponibilidade.

## Componentes do controle de roteamento

O diagrama a seguir ilustra um exemplo de componentes que oferecem suporte ao recurso de controle de roteamento no Route 53 ARC. Os controles de roteamento mostrados aqui agrupados em um painel de controle permitem gerenciar o tráfego para duas zonas de disponibilidade em cada uma das duas regiões. Quando você atualiza os estados de controle de roteamento, o Route 53 ARC altera as verificações de integridade no Amazon Route 53, que redirecionam o tráfego de DNS para células diferentes. As regras de segurança que você configura para controles de roteamento ajudam a evitar cenários de falha aberta e outras consequências não intencionais.




A seguir estão os componentes do atributo de controle de roteamento no Route 53 ARC.

Cluster

Um cluster é um conjunto de cinco endpoints regionais redundantes nos quais você inicia chamadas de API para atualizar ou obter estados de controle de roteamento. Um cluster inclui um painel de controle padrão, e você pode hospedar vários painéis e controles de roteamento em um cluster.

Controles de roteamento

Um controle de roteamento é um simples botão liga-desliga, hospedado em um cluster, que você usa para controlar o roteamento do tráfego do cliente para dentro e fora das células. Ao criar um controle de roteamento, você adiciona uma verificação de integridade no Route 53 ARC. Isso permite que você redirecione o tráfego ao atualizar o estado do controle de roteamento no Route 53 ARC, usando as verificações de integridade configuradas com registros DNS para os aplicativos.

Verificação de integridade do controle de roteamento

Os controles de roteamento são integrados às verificações de integridade no Route 53. As verificações de integridade estão associadas aos registros DNS na frente de cada réplica do aplicativo, por exemplo, os registros de failover. Quando você altera os estados de controle

de roteamento, o Route 53 ARC atualiza as verificações de integridade correspondentes, que redirecionam o tráfego, por exemplo, para fazer o failover da sua réplica em espera.

Painel de controle

Um painel de controle agrupa um conjunto de controles de roteamento relacionados. Você pode associar vários controles de roteamento a um painel de controle e, em seguida, criar regras de segurança para o painel para garantir que as atualizações de redirecionamento de tráfego feitas sejam seguras. Por exemplo, você pode configurar um controle de roteamento para cada um dos balanceadores de carga em cada zona de disponibilidade e, em seguida, agrupá-los no mesmo painel de controle. Em seguida, você pode adicionar uma regra de segurança (uma regra de afirmação) que garanta que pelo menos uma zona (representada por um controle de roteamento) esteja ativa a qualquer momento, para evitar cenários de “falha aberta” não intencionais.

Painel de controle padrão

Quando você cria um cluster, o Route 53 ARC cria um painel de controle padrão. Por padrão, todos os controles de roteamento que você cria no cluster são adicionados ao painel de controle padrão. Ou você pode criar seus próprios painéis de controle para agrupar controles de roteamento relacionados.

Regra de segurança

As regras de segurança são regras que você adiciona ao Route 53 ARC para garantir que as ações de recuperação não prejudiquem acidentalmente a disponibilidade do seu aplicativo. Por exemplo, é possível criar uma regra de segurança que crie um controle de roteamento que atue como uma chave geral liga/desliga para ativar ou desativar um conjunto de outros controles de roteamento.

Endpoint (endpoint do cluster)

Cada cluster no Route 53 ARC tem cinco endpoints regionais que você pode usar para definir e recuperar estados de controle de roteamento. Seu processo de acesso aos endpoints deve assumir que o Route 53 ARC regularmente ativa e desativa os endpoints para manutenção. Portanto, você deve testar cada endpoint sucessivamente até se conectar a um. Acesse os endpoints para obter o estado atual dos controles de roteamento (ligado ou desligado) e acionar failovers para seus aplicativos alterando os estados de controle de roteamento.

# Disponibilidade AWS regional do controlador de recuperação de aplicativos Amazon Route 53

Para obter informações detalhadas sobre endpoints regionais de suporte e serviço para o Controlador de recuperação de aplicações do Amazon Route 53, consulte Endpoints e cotas do Controlador de recuperação de aplicações do Amazon Route 53 na Referência geral da Amazon Web Services.

> **Note**
>
> A verificação de prontidão e o controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53 são atributos globais. No entanto, você deve especificar a região Oeste dos EUA (Oregon) (especificar o parâmetro`--region us-west-2`) nos AWS CLI comandos ARC do Regional Route 53. Isso é válido para a criação de recursos como grupos de recuperação, verificações de prontidão ou clusters.

A mudança de zona no Route 53 ARC está disponível em todas as AWS regiões. Os recursos de controle de roteamento, verificação de prontidão e mudança automática zonal do serviço Route 53 ARC não estão disponíveis nas regiões de Pequim e Ningxia nem em. AWS GovCloud (US)

# Como o Controlador de recuperação de aplicações do Amazon Route 53 funciona

O Controlador de recuperação de aplicações do Amazon Route 53 ajuda você a se preparar e a mitigar rapidamente as deficiências dos aplicativos ativados na AWS.

- Uma verificação de prontidão audita continuamente a capacidade, a configuração, as AWS cotas e as políticas de roteamento dos AWS recursos de um aplicativo e fornece informações que você pode usar para ajudar na recuperação bem-sucedida de falhas no aplicativo. As verificações de prontidão ajudam a garantir que seu ambiente de recuperação seja escalado e configurado para realizar o failover quando necessário.
- Os controles de roteamento permitem que você reequilibre o tráfego entre réplicas de aplicativos durante falhas, para garantir que seu aplicativo esteja disponível. Você também pode combinar controles de roteamento com regras de segurança para evitar consequências não intencionais. Por exemplo, talvez você queira evitar a desativação inadvertida de todos os controles de roteamento

de um aplicativo, o que interromperia todo o fluxo de tráfego, resultando em um cenário de falha aberta.

- Uma mudança de zona transfere temporariamente o tráfego de um recurso para fora de uma zona de disponibilidade (AZ), para que você se recupere de forma rápida e confiável de deficiências em aplicações multi-AZ. Os recursos atualmente suportados são Network Load Balancers e Application Load Balancers com o balanceador de carga entre zonas desativado.

Saiba mais sobre como o Route 53 ARC funciona nas seções a seguir.

-
-
-
-
-

## Monitorar a réplica do aplicativo com verificações de prontidão

O Route 53 ARC audita suas réplicas de aplicativos usando verificações de prontidão para garantir que cada uma tenha a mesma configuração e o mesmo estado de runtime.

Para estar preparado para a recuperação, mantenha capacidade ociosa suficiente em todos os momentos para absorver o tráfego de failover de outra zona ou região de disponibilidade. O Route 53 ARC inspeciona continuamente (uma vez por minuto) seu aplicativo para garantir que a capacidade provisionada corresponda a todas as zonas ou regiões de disponibilidade. A capacidade que o Route 53 ARC inspeciona inclui, por exemplo, contagens de instâncias do Amazon EC2, unidades de capacidade de leitura e gravação do Aurora e tamanho do volume do Amazon EBS. Se você aumentar a capacidade em sua réplica primária para valores de recursos, mas esquecer de aumentar os valores correspondentes em sua réplica em espera, o Route 53 ARC detectará a incompatibilidade para que você possa aumentar os valores na réplica em espera.

> **Important**
>
> As verificações de prontidão são muito úteis para conferir continuamente se as configurações da réplica do aplicativo e os estados de runtime estão alinhados. As verificações de prontidão não devem ser usadas para indicar se sua réplica de produção está íntegra, nem você deve

confiar nas verificações de prontidão como principal gatilho para o failover durante um evento de desastre.

Em uma configuração de espera ativa, você deve tomar decisões sobre se deve falhar de ou para uma célula com base em seus sistemas de monitoramento e verificação de integridade. Considere as verificações de prontidão como um serviço complementar a esses sistemas. As verificações de prontidão do Route 53 ARC não estão altamente disponíveis, portanto, você não deve depender de que as verificações estejam acessíveis durante uma interrupção. Além disso, os recursos verificados também podem não estar disponíveis durante um evento de desastre.

Você pode monitorar o status de prontidão dos recursos do seu aplicativo em células específicas (AWS regiões ou zonas de disponibilidade) ou do aplicativo geral. Você pode ser notificado quando o status de uma verificação de prontidão mudar, por exemplo, para`Not ready`, criando regras em EventBridge. Para ter mais informações, consulte Usando o Route 53 ARC com a Amazon EventBridge. Você também pode visualizar o status de prontidão no AWS Management Console, ou usando operações de API, como`get-recovery-readiness`. Para ter mais informações, consulte Operações de API de prontidão para recuperação (verificação de prontidão).

## Redirecionar o tráfego para recuperação com o controle de roteamento

Um controle de roteamento do Route 53 ARC é um botão liga/desliga que altera o estado de uma verificação de integridade do Route 53 ARC, que pode então ser associada a um registro DNS que redireciona o tráfego, por exemplo, de uma réplica de implantação primária para uma em espera.

Se houver uma falha no aplicativo ou um problema de latência, você pode atualizar os estados do controle de roteamento para transferir o tráfego da sua réplica principal para, por exemplo, uma réplica em espera. Ao usar as operações altamente confiáveis da API do plano de dados do Route 53 ARC para fazer consultas de controle de roteamento e atualizações do estado dele, você pode confiar no Route 53 ARC para o failover durante cenários de recuperação de desastres. Para ter mais informações, consulte Obter e atualizar estados de controle de roteamento usando a API do Route 53 ARC (recomendado).

O Route 53 ARC mantém os estados de controle de roteamento em um cluster, que é um conjunto de cinco endpoints regionais redundantes. O Route 53 ARC propaga as mudanças do estado do controle de roteamento em todo o cluster, que está localizado em uma frota do Amazon EC2, para obter um quórum em cinco regiões. AWS Após a propagação, quando você consulta o Route 53 ARC em busca de um estado de controle de roteamento, usando a API e o plano de dados altamente confiável, ele retorna a visão consensual.

Você pode interagir com qualquer um dos cinco endpoints do cluster para atualizar o estado de um controle de roteamento de, por exemplo, `Off` para `On`. Em seguida, o Route 53 ARC propaga a atualização pelas cinco regiões do cluster.

A consistência dos dados em todos os cinco endpoints do cluster é alcançada em 5 segundos, em média, e após no máximo 15 segundos.

O Route 53 ARC oferece extrema confiabilidade com seu plano de dados para você realizar o failover manual de seu aplicativo entre células. O Route 53 ARC garante que pelo menos três dos cinco endpoints do cluster estejam sempre acessíveis para você realizar alterações no estado do controle de roteamento. Observe que cada cluster do Route 53 ARC é de inquilino único, para garantir que você não seja afetado por “vizinhos barulhentos” que podem retardar seus padrões de acesso.

Ao fazer alterações nos estados de controle de roteamento, você confia nos três critérios a seguir, que provavelmente não falharão:

- Pelo menos três dos seus cinco endpoints estão disponíveis e participam do quórum.
- Você tem credenciais do IAM ativas e pode se autenticar em um endpoint de cluster regional funcional.
- O plano de dados do Route 53 está íntegro (esse plano de dados foi projetado para atender a um SLA de 100% de disponibilidade).

### Resiliência no Route 53 ARC

Aqui está um exemplo de incorporação de controles de roteamento em sua estratégia de failover para melhorar a resiliência e a disponibilidade de seus aplicativos na AWS.

Você pode oferecer suporte a AWS aplicativos de alta disponibilidade AWS executando várias (normalmente três) réplicas redundantes em todas as regiões. Em seguida, é possível usar o controle de roteamento do Amazon Route 53 para encaminhar o tráfego para a réplica apropriada.

Por exemplo, você pode configurar uma réplica de aplicativo para estar ativa e atender ao tráfego de aplicativos, enquanto outra é uma réplica em espera. Quando sua réplica ativa apresenta falhas, você pode redirecionar o tráfego do usuário para lá para restaurar a disponibilidade do aplicativo. As verificações de prontidão podem ajudá-lo a garantir que uma réplica em espera corresponda continuamente à réplica de produção. No entanto, você deve decidir se deseja remover ou corrigir uma réplica com base nas informações de seus sistemas de monitoramento e verificação de

integridade e considerar as verificações de prontidão como um serviço complementar a esses sistemas.

Se você quiser permitir recuperações mais rápidas, outra opção para sua arquitetura é uma implementação ativa-ativa. Com essa abordagem, todas as suas réplicas ficam ativas ao mesmo tempo. Isso significa que você pode se recuperar de falhas afastando os usuários da réplica de seu aplicativo danificado simplesmente redirecionando o tráfego para outra réplica ativa.

## Afastar o tráfego de uma zona de disponibilidade com mudança de zona

Com a mudança zonal, você pode mover o tráfego de um recurso de balanceamento de carga para fora de uma Zona de Disponibilidade (AZ), para que você possa continuar operando seu aplicativo normalmente nas outras AZs em uma região. AWS Você pode iniciar uma mudança de zona para Network Load Balancers e Application Load Balancers com o balanceamento de carga entre zonas desativado.

Quando você implanta e executa AWS aplicativos em balanceadores de carga em várias (normalmente três) AZs em uma região, você pode recuperar rapidamente um aplicativo em uma AZ prejudicada iniciando uma mudança de zona. A transferência do tráfego da aplicação para outras AZs reduz a duração e a gravidade do impacto causado por quedas de energia ou problemas de hardware ou software na AZ.

Quando você inicia uma mudança de zona para uma AZ, o Route 53 ARC define as verificações de integridade do Amazon Route 53 como não íntegras para os endereços IP correspondentes do recurso de balanceador de carga, de forma que o tráfego do recurso não seja mais direcionado para a AZ. Quando a mudança de zona expira ou você a cancela, o Route 53 ARC define as verificações de integridade do Route 53 como íntegras novamente e os endereços IP de zona originais são restaurados.

Uma mudança de zona deve ter uma data de expiração, quando o tráfego retornará à AZ. Inicialmente, você pode definir uma mudança de zona para expirar em no máximo três dias (72 horas). No entanto, você pode atualizar uma mudança de zona para definir uma nova expiração a qualquer momento (o que, no entanto, ainda tem duração máxima de três dias). Você também pode cancelar uma mudança de zona antes que ela expire, se estiver pronto para restaurar o tráfego para o AZ mais cedo.

Em alguns cenários específicos, a mudança de zona não desloca o tráfego da AZ. Por exemplo, se os grupos de destino do balanceador de carga nas AZs não tiverem nenhuma instância ou se

nenhuma das instâncias estiverem íntegras, o balanceador de carga estará em um estado de falha aberta e você não poderá transferir uma das AZs.

Para saber mais sobre a mudança de zona, consulte Mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53.

## AWS afasta o tráfego de uma zona de disponibilidade com mudança automática zonal

O deslocamento automático zonal é um recurso que AWS retira o tráfego de recursos do aplicativo de uma zona de disponibilidade, em seu nome. AWS inicia um deslocamento automático quando a telemetria interna indica que há uma deficiência na zona de disponibilidade que pode afetar potencialmente os clientes. A telemetria interna incorpora métricas de várias fontes, incluindo a AWS rede e os serviços Amazon EC2 e Elastic Load Balancing.

Você pode habilitar a mudança automática de zona para Network Load Balancers e Application Load Balancers com o balanceamento de carga entre zonas desativado.

Quando você implanta e executa AWS aplicativos em balanceadores de carga em várias (normalmente três) AZs em uma região e pré-dimensiona para oferecer suporte à estabilidade estática, é AWS possível recuperar rapidamente os aplicativos do cliente em uma AZ transferindo o tráfego com um deslocamento automático. Ao transferir o tráfego de recursos para outras AZs na região, é AWS possível reduzir a duração e a gravidade do impacto potencial causado por quedas de energia, problemas de hardware ou software em uma AZ ou outras deficiências.

Quando AWS inicia um deslocamento automático para um recurso de balanceamento de carga, o Route 53 ARC define as verificações de saúde do Amazon Route 53 como não íntegras para os endereços IP correspondentes do recurso de balanceador de carga, de forma que o tráfego do recurso não seja mais direcionado para a AZ. Quando AWS determina que o AZ está pronto para o retorno do tráfego do aplicativo, o Route 53 ARC restaura as verificações de integridade do Route 53 e os endereços IP zonais originais são restaurados.

Ao habilitar a mudança automática de zona para um recurso, você também deve configurar uma execução prática para o recurso. A AWS realiza execuções práticas cerca de uma vez por semana, durante 30 minutos, para ajudar a garantir que você a aplicação sem uma das zonas de disponibilidade da região.

Assim como no caso da mudança de zona, há alguns cenários específicos em que a mudança automática de zona não transfere o tráfego para fora da AZ. Por exemplo, se os grupos de destino do balanceador de carga nas AZs não tiverem nenhuma instância ou se nenhuma das instâncias

estiverem íntegras, o balanceador de carga estará em um estado de falha aberta e você não poderá transferir uma das AZs.

Para saber mais sobre a mudança automática de zona, consulte Mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53.

## Planos de controle e planos de dados para o Route 53 ARC

Ao planejar o failover e a recuperação de desastres, é importante considerar a resiliência de seus mecanismos de failover e garantir que os mecanismos dos quais você depende estejam altamente disponíveis, para usá-los quando preciso em um cenário de desastre. Normalmente, você deve usar funções de plano de dados para seus mecanismos quando puder, para obter a maior confiabilidade e tolerância a falhas. Com isso em mente, é importante entender como a funcionalidade de um serviço é dividida entre planos de controle e planos de dados e quando você pode confiar em uma expectativa de extrema confiabilidade com o plano de dados de um serviço.

O Route 53 ARC inclui dois conjuntos de funcionalidades, verificações de prontidão e controle de roteamento para recuperação. Como acontece com a maioria dos AWS serviços, a funcionalidade ARC do Route 53 é suportada por planos de controle e planos de dados. 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. Um plano de dados é projetado para ser resistente e manter a disponibilidade mesmo durante eventos de ruptura, quando um plano de controle pode ficar indisponível. Por isso, recomendamos que você use operações de plano de dados quando a disponibilidade for importante, por exemplo, quando precisar redirecionar o tráfego para uma réplica em espera durante uma interrupção.

Em geral, um plano de controle permite que você execute funções básicas de gerenciamento, como criar, atualizar e excluir recursos no serviço. Um plano de dados fornece a funcionalidade principal de um serviço.

Para o Route 53 ARC, os planos de controle e os planos de dados são divididos da seguinte forma:

- Para mudanças de zona, os recursos suportados são registrados automaticamente no Route 53 ARC. Quando um recurso é registrado, ele se torna um recurso gerenciado para mudanças de zona no Route 53 ARC. O Route 53 ARC tem um plano de dados em cada AWS região que fornece operações de API para obter, listar, criar e atualizar mudanças de zona para recursos gerenciados. O plano de dados de mudança de zona está altamente disponível.
- Para verificações de prontidão, há uma única API, a API de prontidão de recuperação, tanto para o plano de controle quanto para o plano de dados. As verificações de prontidão e os recursos de

preparação estão disponíveis apenas na região Oeste dos EUA (Oregon, us-west-2). O plano de controle e o plano de dados das verificações de prontidão não estão altamente disponíveis.

- Para controle de roteamento, a API do plano de controle é a API de Configuração do controle de recuperação, com suporte na região Oeste dos EUA (Oregon, us-west-2). Você usa essas operações de API ou as AWS Management Console para criar ou excluir clusters, painéis de controle e controles de roteamento, para ajudar a se preparar para um evento de recuperação de desastres quando talvez seja necessário redirecionar o tráfego para seu aplicativo. O plano de controle da configuração do controle de roteamento não é altamente disponível.
- O plano de dados de controle de roteamento no Route 53 ARC é um cluster dedicado em cinco regiões geograficamente isoladas da AWS . Cada cliente cria um ou mais clusters usando o plano de controle de roteamento. O cluster hospeda painéis de controle e controles de roteamento. Em seguida, você usa a API de controle de roteamento (cluster de recuperação) para obter, listar e atualizar os estados do controle de roteamento quando quiser redirecionar o tráfego para o aplicativo. O plano de dados de controle de roteamento é altamente disponível.

Para saber mais sobre a preparação para a recuperação e a preparação para o failover com o Route 53 ARC, consulte Práticas recomendadas para o Controlador de recuperação de aplicações do Amazon Route 53.

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.

# Comparar mudanças de zona e controles de roteamento no Controlador de recuperação de aplicações do Amazon Route 53

A mudança zonal, incluindo a mudança automática zonal, e o controle de roteamento no Amazon Route 53 Application Recovery Controller podem alcançar uma recuperação rápida e ajudar a manter a resiliência dos aplicativos. AWS Ambas as opções estão altamente disponíveis e ajudam a apoiar a recuperação em cenários com maior latência ou disponibilidade reduzida. Ambos também permitem que você recupere aplicações rapidamente ao mover o tráfego, limitando o impacto e o tempo perdido com deficiências.

O controle de roteamento se concentra principalmente em AWS aplicativos que estão em várias AWS regiões, enquanto o deslocamento zonal e o deslocamento automático zonal só oferecem

suporte a AWS aplicativos com balanceadores de carga em implantações de zona de disponibilidade múltipla (Multi-AZ). Também há outras diferenças, como descrito nesta seção.

As informações na tabela a seguir incluem alguns dos principais recursos da mudança de zona, da mudança automática de zona e do controle de roteamento, além de informações sobre comparação entre as opções. Essas descrições podem ajudar você a entender melhor como opções diferentes podem ser a melhor opção para as necessidades de recuperação de desastres da sua organização.

| Controle de roteamento | Mudança de zona | Mudança automática de zona |
| --- | --- | --- |
| Regional<br><br>Redireciona o tráfego de uma AWS região para outra (principalmente)<br><br>Também pode ser usada para redirecionar entre zonas de disponibilidade | De zona<br><br>Afasta o tráfego de uma zona de disponibilidade<br><br>O tráfego vai para outras zonas de disponibilidade na região, não para um destino específico | De zona<br><br>Afasta o tráfego de uma zona de disponibilidade<br><br>O tráfego vai para outras zonas de disponibilidade na região, não para um destino específico |
| Requer configuração<br><br>Requer configuração e setup | Disponível sem setup<br><br>Ativado automaticamente pelos serviços compatíveis<br><br>(atualmente, Application Load Balancer e Network Load Balancer) | Requer configuração de execução prática<br><br>Disponível para serviços compatíveis<br><br>(atualmente, Application Load Balancer e Network Load Balancer) |
| Iniciada pelo cliente<br><br>O cliente determina quando redirecionar o tráfego | Iniciada pelo cliente<br><br>O cliente determina quando iniciar uma mudança de zona | Iniciada pela AWS<br><br>AWS afasta o tráfego do aplicativo de uma AZ em seu nome |
| Com base em taxas<br><br>Requer cobranças separadas para controle de roteamento | Incluído nos serviços<br><br>A criação de mudanças de zona para transferir o | Incluído nos serviços<br><br>A inicialização de mudanças automáticas para transferir |

| Controle de roteamento | Mudança de zona | Mudança automática de zona |
| --- | --- | --- |
| | tráfego para fora das AZs está incluída nos balanceadores de carga compatíveis | o tráfego para fora das AZs em seu nome está incluída nos balanceadores de carga compatíveis |
| Não expira | Temporária | Temporária |
| O tráfego pode ser redirecionado para uma réplica indefinidamente | Todas as mudanças de zona devem ser configuradas para expirar | AWS inicia e termina os turnos automáticos |

Para saber mais sobre cada um desses recursos, consulte os seguintes capítulos:

- Mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53
- Mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53
- Controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53

# Casos de uso do Controlador de recuperação de aplicações do Amazon Route 53

Durante uma falha, você pode usar o controle de roteamento e a mudança de zona para garantir que o tráfego rapidamente restaure a disponibilidade do aplicativo.

O atributo de controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53 foi projetado para empresas que têm aplicativos com requisitos de disponibilidade extremamente altos, como um objetivo de tempo de recuperação (RTO) de menos de cinco minutos ou um requisito de disponibilidade maior que 99,99%. As aplicações típicas incluem sistemas nacionais de autenticação de pagamentos, processamento de pagamentos em tempo real ou cargas de trabalho de negociação de ações que podem ter um amplo impacto financeiro se falharem. Talvez seja necessário que esses aplicativos se protejam até mesmo contra falhas parciais, como um aumento de milissegundos na latência ou uma taxa de erro de 5%.

Um caso de uso corporativo da mudança de zona do Route 53 ARC é gerenciar a recuperação de zonas de multidisponibilidade, para se proteger contra falhas comuns de aplicativos, como uma implantação incorreta em uma única zona de disponibilidade. Com o deslocamento automático

zonal, AWS afasta o tráfego de uma AZ para um recurso quando AWS determina que há um possível problema na AZ que pode afetar adversamente os aplicativos do cliente. Outro caso de uso corporativo para controle de roteamento é a recuperação entre regiões, em que uma organização deseja se recuperar de um evento de grande escala, como um desastre natural, e supervisionar a recuperação centralmente.

Para resumir, o Route 53 ARC oferece os seguintes benefícios:

- Sem configuração inicial, você pode usar mudanças de zona para mitigar falhas parciais do aplicativo, retirando rapidamente o tráfego de um balanceador de carga de uma zona de disponibilidade para se recuperar temporariamente e com confiabilidade de um problema. Isso lhe dá tempo para investigar, enquanto seu aplicativo continua sendo executado nas outras zonas de disponibilidade.
- Depois de configurar uma prática, execute e habilite o deslocamento automático zonal, para que o tráfego de AWS turnos afaste do tráfego, em seu nome. AWS inicia um deslocamento automático quando a telemetria interna indica que há uma deficiência na zona de disponibilidade que pode afetar potencialmente os clientes. AWS para de mudar o tráfego quando um AZ se recupera. Você não precisa decidir quando transferir o tráfego de uma AZ; AWS usa seus sinais internos para decidir quando tomar medidas de mitigação. Enquanto AWS investiga e resolve a deficiência do AZ, seu aplicativo continua sendo executado nas outras zonas de disponibilidade da região.
- Se você configurou o controle de roteamento, pode responder aos estados de falha parcial usando o Route 53 ARC de maneiras que os sistemas de recuperação automatizados talvez não consigam. Por exemplo, depois de configurar o controle de roteamento no Route 53 ARC, você pode configurar um CloudWatch alarme da Amazon ou uma verificação de saúde do Amazon Route 53 para responder a um aumento de milissegundos na latência ou a um aumento de 5% nas taxas de erro redirecionando o tráfego usando os controles de roteamento ARC do Route 53.
- Você pode usar verificações de prontidão para monitorar, de forma contínua, as alterações na capacidade e na configuração em todas as réplicas para ajudar a garantir que você esteja preparado e escalado para lidar com failovers.
- Você pode receber recomendações sobre como melhorar a capacidade de recuperação de sua arquitetura existente para criar um design de aplicativo mais confiável.

# Atribuição de tags no Controlador de recuperação de aplicações do Amazon Route 53

As tags são palavras ou frases (metadados) que você usa para identificar e organizar seus AWS recursos. É possível adicionar várias tags a cada recurso, e cada tag inclui uma chave e um valor definidos por você. Por exemplo, a chave pode ser o ambiente e o valor pode ser a produção. Você pode pesquisar e filtrar seus recursos de acordo com as tags que adicionar.

Você pode marcar os seguintes recursos:

- Grupos de recuperação
- Células
- Conjuntos de recursos
- Verificação de prontidão
- Clusters
- Painéis de controle
- Regras de segurança no controle de roteamento

A marcação no Route 53 ARC está disponível somente por meio da API, por exemplo, usando a AWS CLI.

A seguir estão exemplos de marcação no Route 53 ARC usando a AWS CLI.

Criar recursos com tags

```
aws route53-recovery-readiness --region us-west-2 create-cell --cell-name
pdx_cell --tags Region=PDX,Stage=Prod
```

```
aws route53-recovery-readiness --region us-west-2 create-recovery-group --
recovery-group-name pdx_recovery_group --tags Region=PDX,Stage=Prod
```

```
aws route53-recovery-readiness --region us-west-2 create-resource-
set --resource-set-name dynamodb_resource_set --resource-set-type
AWS::DynamoDB::Table --resources ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/PDXCell,ResourceArn=arn:aws:dynamodb:us-
west-2:111122223333:table/PDX_Table ReadinessScopes=arn:aws:aws-recovery-
```

```
readiness::111122223333:cell/IADCell,ResourceArn=arn:aws:dynamodb:us-
east-1:111122223333:table/IAD_Table --tags Stage=Prod

aws route53-recovery-readiness --region us-west-2 create-readiness-
check --readiness-check-name dynamodb_readiness_check --resource-set-name
dynamodb_resource_set --tags Stage=Prod

aws route53-recovery-control-config --region us-west-2 create-cluster --
cluster-name example1-cluster --tags Region=PDX,Stage=Prod

aws route53-recovery-control-config --region us-west-2 create-control-panel
--control-panel-name example1-control-panel --cluster-arn arn:aws:route53-
recovery-control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
--tags Region=PDX,Stage=Prod
```

Marcar e desmarcar os recursos existentes

```
aws route53-recovery-readiness --region us-west-2 tag-resource --resource-
arn arn:aws:aws-recovery-readiness::111122223333:cell/MyCell --tags
Owner=DevOps

aws route53-recovery-readiness --region us-west-2 untag-resource --
resource-arn arn:aws:aws-recovery-readiness::111122223333:cell/MyCell --
tag-keys Owner
```

Para obter mais informações, consulte TagResourceo Guia de referência da API Recovery Readiness para o Amazon Route 53 Application Recovery Controller e TagResourceo Guia de referência da API de configuração de controle de recuperação do Amazon Route 53 Application Recovery Controller.

# Preços do Controlador de recuperação de aplicações do Amazon Route 53

Com o Controlador de recuperação de aplicações do Amazon Route 53, você paga apenas pelo que configurar para usar no serviço. A seguir está um resumo de como os preços funcionam para o Route 53 ARC:

- Para mudanças de zona: você pode usar uma mudança de zona para recuperar seu aplicativo de um problema em uma zona de disponibilidade. Não há cobrança adicional pelo uso da mudança de zona.

- Para mudança automática zonal: AWS afasta o tráfego de uma zona de disponibilidade em seu nome quando AWS determina que há um problema potencial que pode afetar adversamente os aplicativos do cliente. Não há nenhuma cobrança adicional pela habilitação da mudança automática de zona.
- Para verificações de prontidão: você paga um custo por hora por verificação de prontidão configurada.
- Para clusters: você paga um custo por hora por cluster criado. Cada cluster pode hospedar vários controles de roteamento, que você usa para acionar failovers de aplicativos.

Para obter informações detalhadas sobre preços e exemplos, consulte Preços do controlador de recuperação de aplicações do Amazon Route 53 e role a tela para baixo até o Amazon Route 53.

# Conceitos básicos da recuperação multirregião no Controlador de recuperação de aplicações do Amazon Route 53

Para usar o Controlador de recuperação de aplicações do Amazon Route 53 com aplicativos da AWS que estão em várias regiões da AWS, há diretrizes a serem seguidas para configurar seus aplicativos para que estejam prontos para recuperação. Em seguida, você pode criar verificações de prontidão para seu aplicativo e configurar controles de roteamento para redirecionar o tráfego para failover. Você também pode revisar as recomendações que o Route 53 ARC fornece sobre a arquitetura do seu aplicativo que pode melhorar a resiliência.

> **Note**
>
> Nenhuma configuração é necessária para usar a mudança de zona do Route 53 ARC para recuperar de forma confiável os aplicativos das deficiências da zona de disponibilidade. Para afastar o tráfego de uma zona de disponibilidade para recursos de balanceador de carga que foram registrados no Route 53 ARC, inicie uma mudança de zona no console do Route 53 ARC ou do Elastic Load Balancing, ou use a AWS Command Line Interface ou AWS SDK com ações da API de mudança de zona. Para ter mais informações, consulte Mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53.

Ao usar o controle de roteamento do Route 53 ARC para se recuperar de falhas de aplicativos, recomendamos que você configure pelo menos duas (normalmente três) réplicas de aplicativos, ou células. Cada célula representa uma região AWS ou zona de disponibilidade. Depois de configurar os recursos do aplicativo em células que se alinham às zonas de disponibilidade em uma região, há algumas etapas adicionais, listadas aqui, que você deve seguir para garantir que seu aplicativo siga um design orientado à recuperação. Depois de implementar essas etapas, você pode usar o Route 53 ARC para o failover entre zonas de disponibilidade.

> **Tip**
>
> Para ajudar a simplificar a configuração, fornecemos AWS CloudFormation modelos do HashiCorp Terraform que criam um aplicativo com réplicas redundantes que falham

independentemente umas das outras. Saiba mais e baixe os modelos em Prontidão para recuperação com um novo aplicativo.

Para se preparar para usar o Route 53 ARC, configure um processo de recuperação resiliente para seu aplicativo. As etapas a seguir são uma visão geral de como você pode preparar seu ambiente de aplicativos para usar o Route 53 ARC:

1. Implante cópias independentes de sua pilha de aplicativos (camada de rede e computação) como réplicas em espera para que você possa fazer o failover do tráfego nas pilhas. Não deve haver nenhuma dependência entre células no código do aplicativo em que a falha de uma célula afetaria outras. Para fazer o failover entre zonas de disponibilidade ou regiões da AWS, os limites de suas células devem estar alinhados com as construções de infraestrutura isoladas na AWS (zonas de disponibilidade ou regiões da AWS). No entanto, se você não configurar seus limites para se alinharem às zonas de disponibilidade ou regiões da AWS, o Route 53 ARC ainda oferecerá suporte ao failover entre células.
2. Replique todos os dados de estado necessários nas células. Você pode usar serviços da AWS de banco de dados para ajudar a replicar seus dados. Por exemplo, para alta disponibilidade, você pode adicionar réplicas de leitura para instâncias do Aurora em todas as zonas de disponibilidade. Durante o failover, você pode então promover uma réplica para ser a instância primária do banco de dados.
3. Configure cada célula para expor um nome de domínio DNS. O nome de domínio deve representar o recurso da AWS de nível superior na célula e atuar como porta de entrada para atender às solicitações do cliente para essa célula. Um recurso de nível superior pode ser, por exemplo, um balanceador de carga do Elastic Load Balancing ou uma API do API Gateway. Independente do recurso ao qual você adicionar o nome, o nome de domínio só deve direcionar solicitações para a infraestrutura dentro da célula.
4. Para ajudá-lo a determinar a melhor estrutura para seu aplicativo, o Route 53 ARC pode executar uma análise e fornecer recomendações de arquitetura. No AWS Management Console, forneça o nome de domínio do aplicativo e outras informações. O Route 53 ARC fornecerá sugestões de arquitetura para uma estrutura que permita a recuperação rápida e completa do failover. Para ter mais informações, consulte Obter recomendações de arquitetura no Route 53 ARC.
5. Para que o failover de tráfego que usa o Route 53 ARC não crie problemas de consistência de dados, projete uma lógica de reconciliação de dados em sua região de failover para failovers regionais de aplicativos com estado que exijam consistência estrita.

As seções a seguir incluem informações mais detalhadas sobre como começar a usar o Route 53 ARC, dependendo se você tem um aplicativo existente ou se está configurando um novo aplicativo.

- Prontidão de recuperação com um aplicativo existente
- Prontidão para recuperação com um novo aplicativo
- Controle de roteamento para failover de tráfego

Para obter mais informações sobre como trabalhar com o Route 53 ARC, consulte:

- Para saber mais sobre os recursos do Route 53 ARC, consulte Verificação de prontidão do Controlador de recuperação de aplicações do Amazon Route 53 e Controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53.
- Para ver exemplos de uso do Route 53 ARC com a AWS CLI, consulte Exemplos de uso das operações da API do Route 53 ARC com a AWS CLI.
- Para ver informações e exemplos do uso da API do Route 53 ARC com AWS SDKs, consulte Usar o Route 53 ARC com um AWS SDK e Exemplos de código para o Application Recovery Controller usando AWS SDKs.
- Para ver uma lista das operações da API do Route 53 ARC, consulte Operações de API comuns para o Controlador de Recuperação de Aplicações do Amazon Route 53.

# Prontidão de recuperação com um aplicativo existente

Com o Controlador de recuperação de aplicações do Amazon Route 53, você pode entender a prontidão de recuperação do seu aplicativo e se preparar para o failover. Se você tiver um aplicativo existente, siga as etapas a seguir antes de configurar o Route 53 ARC para ele:

- Identifique o aplicativo que você deseja configurar com prontidão para recuperação.
- Analise as definições dos componentes no Route 53 ARC. Para ter mais informações, consulte Componentes da verificação de prontidão .
- Primeiramente, revise as informações em Prontidão para recuperação com um novo aplicativo.
- Configure os usuários, as funções e as políticas necessários para o Route 53 ARC. Para ter mais informações, consulte Segurança no Controlador de recuperação de aplicações do Amazon Route 53.

Para configurar a estrutura que permite a prontidão para recuperação no Route 53 ARC, você pode usar a API do Route 53 ARC, por exemplo, usando a AWS CLI ou o AWS Management Console. Você também pode usar AWS CloudFormation nossos modelos do HashiCorp Terraform para começar rapidamente com o Route 53 ARC.

Com uma dessas opções, você modela réplicas ou unidades de contenção de falhas para seu aplicativo. Em cada réplica, você define os recursos que seu aplicativo usará, como grupos e balanceadores de carga do Amazon EC2 Auto Scaling. Você pode entender a prontidão para recuperação do seu aplicativo como um todo ou como réplicas individuais dentro do seu aplicativo. Você pode ver o status de prontidão usando ações de API, como `get-recovery-readiness`, ou revisando o status de prontidão no console. Para ter mais informações, consulte Monitorar o status de prontidão no Route 53 ARC.

Se você já tem um aplicativo para o qual deseja configurar verificações de prontidão, o Route 53 ARC pode analisar a configuração dele e fornecer orientações específicas sobre como torná-lo mais orientado à recuperação. Para ter mais informações, consulte Obter recomendações de arquitetura no Route 53 ARC.

O Route 53 ARC também verifica continuamente suas arquiteturas de aplicativos e políticas de roteamento do Amazon Route 53 para detectar problemas. Para ter mais informações, consulte Verificações de prontidão de recursos de destino do DNS: auditando a prontidão de resiliência.

## Prontidão para recuperação com um novo aplicativo

Se você estiver projetando um novo aplicativo, estruture-o para ser orientado à recuperação desde o início, para aproveitar ao máximo os recursos de recuperação do Controlador de recuperação de aplicações do Amazon Route 53.

Um aplicativo orientado à recuperação consiste em várias réplicas redundantes, ou unidades de contenção de falhas, que falham independentemente umas das outras. Configure silos de contenção de falhas implantando réplicas que se alinham aos limites da zona de disponibilidade da AWS. Isso é mais fácil se você estiver começando um novo aplicativo do que se precisar redefinir a arquitetura de um existente.

As seções a seguir incluem um exemplo que ilustra projetar um aplicativo orientado à recuperação com réplicas em silos em zonas de disponibilidade da AWS. O exemplo usa AWS CloudFormation modelos para simplificar o processo, bem como modelos disponíveis para download AWS CloudFormation e do HashiCorp Terraform com um aplicativo de amostra para que você mesmo possa explorar rapidamente a configuração e o uso do Route 53 ARC.

Tópicos



## Como criar um aplicativo de exemplo

Como exemplo, vejamos um aplicativo que direciona o tráfego para um serviço que é executado no Amazon Elastic Container Service (Amazon ECS), é liderado por um Network Load Balancer e interage com um banco de dados Amazon Aurora. Você pode iniciar esse aplicativo com um modelo do AWS CloudFormation e provisioná-lo como uma pilha.

Para garantir que você implante réplicas em silos, cada uma com escopo definido em uma zona de disponibilidade, faça o seguinte: certifique-se de que a arquitetura do seu aplicativo use um Network Load Balancer local para uma réplica que é roteada para um cluster do Amazon ECS, que também é local para a réplica. Conecte essas réplicas usando um registro DNS da política de roteamento ponderado do Amazon Route 53. Em seguida, defina pilhas separadas para cada réplica em um único modelo AWS CloudFormation usando parâmetros no modelo. Saiba mais sobre o uso de estruturas aninhadas do AWS CloudFormation lendo Como trabalhar com pilhas aninhadas no Guia do usuário do AWS CloudFormation.

Você pode criar o aplicativo no AWS CloudFormation seguindo estas etapas:

1. Crie um modelo principal que defina seus serviços da AWS gerenciados em cada região da AWS, mas não em cada zona de disponibilidade. Inclua, por exemplo, tabelas regionais do Aurora ou buckets do Amazon S3 adicionais às réplicas criadas em cada zona de disponibilidade. Será necessário exportar esses recursos.
2. Em outro modelo, defina os recursos da AWS que têm como escopo uma réplica, como Network Load Balancers que têm como escopo uma zona de disponibilidade. Esses recursos devem usar parâmetros de modelo para propriedades de configuração de recursos diferentes em cada réplica.
3. Crie cada réplica usando o modelo de réplica e transmita os parâmetros ou importe valores do modelo principal.

Ao usar infrastructure-as-code recursos que oferecem suporte à infraestrutura de provisionamento com base em parâmetros dinâmicos, você pode reutilizar as definições em seu modelo. AWS CloudFormation Você pode ver isso ilustrado nos exemplos de modelos do AWS CloudFormation para download que fornecemos na próxima seção. O uso de parâmetros permite definir um aplicativo

que se alinha aos padrões de design focados na região no Route 53 ARC, para que seu aplicativo seja mais resiliente usando aproximadamente o mesmo número de definições em seu modelo.

## Baixe nossos AWS CloudFormation modelos do HashiCorp Terraform

Para ajudar você a começar a usar o Route 53 ARC, fornecemos AWS CloudFormation modelos do HashiCorp Terraform, junto com um exemplo de aplicativo e step-by-step instruções, que você pode baixar e implantar localmente.

Depois de implantar o aplicativo de exemplo, você pode usar os modelos para criar componentes do Route 53 ARC e, em seguida, explorar o uso de controles de roteamento para gerenciar o fluxo de tráfego para o aplicativo. Você pode adaptar os modelos e o processo para seu próprio cenário e aplicativos.

- AWS CloudFormation: para começar a usar um aplicativo e modelos do AWS CloudFormation de exemplo, consulte as instruções do README neste bucket do Amazon S3. Você pode aprender mais sobre o uso de modelos do AWS CloudFormation lendo Conceitos do AWS CloudFormation no Guia do usuário do AWS CloudFormation.
- HashiCorp Terraform: Para começar a usar um aplicativo de amostra e modelos do Terraform, consulte as instruções do README aqui neste bucket do Amazon S3. Você pode aprender mais sobre como usar os modelos do Terraform lendo a HashiCorp documentação.

# Controle de roteamento para failover de tráfego

O recurso de controle de roteamento do Controlador de recuperação de aplicações do Amazon Route 53 aciona failovers de tráfego entre cópias redundantes de aplicativos, ou réplicas, executadas em distintas regiões ou zonas de disponibilidade da AWS. Para acionar failover associe os controles de roteamento do Route 53 ARC aos nomes de domínio de nível superior das réplicas. Em seguida, adicione uma verificação de integridade do controle de roteamento para controlar o roteamento de tráfego nas réplicas do aplicativo. Você pode atualizar os estados de controle de roteamento no AWS Management Console, mas recomendamos que você use as ações do Route 53 ARC, usando a API ou a AWS CLI, para atualizar os estados de controle de roteamento.

Por exemplo, se quiser fazer o failover entre as zonas de disponibilidade us-west-1a e us-west-1b, use a ação da `update-routing-control-state` API para definir o estado de `us-east-1a` para `Off` e `us-east-1b` para `On`.

Para obter mais informações sobre a configuração e o uso do controle de roteamento no Route 53 ARC, consulte Controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53.

# Usar o Route 53 ARC com um AWS SDK

Os kits de desenvolvimento de software (SDKs) da AWS 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++ | Exemplos de código do AWS SDK for C++ |
| AWS SDK for Go | Exemplos de código do AWS SDK for Go |
| AWS SDK for Java | Exemplos de código do AWS SDK for Java |
| AWS SDK for JavaScript | Exemplos de código do AWS SDK for JavaScript |
| AWS SDK para Kotlin | Exemplos de código do AWS SDK para Kotlin |
| AWS SDK for .NET | Exemplos de código do AWS SDK for .NET |
| AWS SDK for PHP | Exemplos de código do AWS SDK for PHP |
| AWS SDK for Python (Boto3) | Exemplos de código do AWS SDK for Python (Boto3) |
| AWS SDK for Ruby | Exemplos de código do AWS SDK for Ruby |
| AWS SDK para Rust | Exemplos de código do AWS SDK para Rust |
| SDK da AWS para SAP ABAP | Exemplos de código do SDK da AWS para SAP ABAP |
| AWS SDK for Swift | Exemplos de código do AWS SDK for Swift |

Para obter exemplos específicos do Route 53 ARC, consulte Exemplos de código para o Application Recovery Controller usando AWS SDKs.

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

# Exemplos de uso das operações da API do Route 53 ARC com a AWS CLI

Esta seção mostra exemplos simples de aplicativos, usando a AWS Command Line Interface para trabalhar com os atributos do Controlador de recuperação de aplicações do Amazon Route 53 usando operações de API. Os exemplos têm como objetivo ajudar a desenvolver uma compreensão básica de como trabalhar com o Route 53 ARC usando a CLI.

Tópicos



## Comece com a verificação de prontidão usando a AWS CLI

A verificação de prontidão no Controlador de recuperação de aplicações do Amazon Route 53 permite que você verifique se os atributos em seus aplicativos estão prontos para o failover.

Vejamos um caso simples em que você tem um aplicativo chamado Simple-Service que atualmente é executado na região Leste dos EUA (Norte da Virgínia, us-east-1). Você também tem uma cópia em espera da aplicação na região Oeste dos EUA (Oregon, us-west-2). Neste exemplo, configuraremos as verificações de prontidão para comparar essas duas versões do aplicativo. Isso nos permite garantir que a região de espera, Oeste dos EUA (Oregon), esteja pronta para receber tráfego, se necessário, em um cenário de failover.

Para obter informações sobre como usar a AWS CLI, consulte a Referência de comandos da AWS CLI. Para conferir uma lista de ações da API de prontidão e links para mais informações, consulte Operações de API de prontidão para recuperação (verificação de prontidão).

As células no Route 53 ARC representam limites de falhas (como zonas de disponibilidade ou regiões) e são coletadas em grupos de recuperação. Um grupo de recuperação representa um aplicativo que você deseja verificar se está pronto para o failover. Para obter mais informações sobre os componentes das verificações de prontidão, consulte Componentes da verificação de prontidão .

> **Note**
>
> O Route 53 ARC é um serviço global que oferece suporte a endpoints em várias Regiões da AWS, mas você deve especificar a região Oeste dos EUA (Oregon), ou seja, especificar o parâmetro `--region us-west-2`, na maioria dos comandos da CLI do Route 53 ARC. Por exemplo, para criar atributos como grupos de recuperação, verificações de prontidão ou clusters.
> Quando você cria um cluster, o Route 53 ARC fornece um conjunto de endpoints regionais. Para obter ou atualizar os estados de controle de roteamento, você deve especificar o endpoint regional (a Região da AWS e a URL do endpoint) em seu comando na CLI.

Para nosso exemplo de aplicação, começaremos criando uma célula para cada região em que temos atributos. Em seguida, criaremos um grupo de recuperação e concluiremos a configuração para uma verificação de prontidão.

## 1. Criar células

1a. Crie uma célula us-east-1.

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name east-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
    "CellName": "east-cell",
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1b. Crie uma célula us-west-1.

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name west-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell",
    "CellName": "west-cell",
```

```
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1c. Agora temos duas células. Você pode verificar se elas existem chamando a API `list-cells`.

```
aws route53-recovery-readiness --region us-west-2 list-cells
```

```
{
    "Cells": [
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell",
            "CellName": "east-cell",
            "Cells": [],
            "ParentReadinessScopes": [],
            "Tags": {}
        },
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell",
            "CellName": "west-cell"
            "Cells": [],
            "ParentReadinessScopes": [],
            "Tags": {}
        }
    ]
}
```

## 2. Criar um grupo de recuperação

Os grupos de recuperação são o atributo de alto nível para prontidão para recuperação no Route 53 ARC. Um grupo de recuperação representa um aplicativo como um todo. Nesta etapa, criaremos um grupo de recuperação para modelar um aplicativo geral e, em seguida, adicionaremos as duas células que criamos.

2a. Criar um grupo de recuperação.

```
aws route53-recovery-readiness --region us-west-2 create-recovery-group \
    --recovery-group-name simple-service-recovery-group \
       --cells "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"\
```

```
        "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
```

```
{
    "Cells": [],
    "RecoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/simple-service-recovery-group",
    "RecoveryGroupName": "simple-service-recovery-group",
    "Tags": {}
}
```

2b. (Opcional) Você pode verificar se seu grupo de recuperação foi criado corretamente chamando a API `list-recovery-groups` .

```
aws route53-recovery-readiness --region us-west-2 list-recovery-groups
```

```
{
    "RecoveryGroups": [
        {
            "Cells": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
            "RecoveryGroupArn": "arn:aws:route53-recovery-
readiness::111122223333:recovery-group/simple-service-recovery-group",
            "RecoveryGroupName": "simple-service-recovery-group",
            "Tags": {}
        }
    ]
}
```

Agora que temos um modelo para nosso aplicativo, vamos adicionar os atributos a serem monitorados. No Route 53 ARC, um grupo de atributos que você deseja monitorar é chamado de conjunto de atributos. Os conjuntos de atributos contêm atributos que são todos do mesmo tipo. Comparamos os atributos em um conjunto de atributos entre si para ajudar a determinar a prontidão de uma célula para o failover.

## 3. Criar um conjunto de atributos.

Vamos supor que nosso aplicativo Simple-Service seja realmente muito simples e use apenas tabelas do DynamoDB. Ele tem uma tabela do DynamoDB em us-east-1 e outra em us-west-2. Um

conjunto de atributos também contém um escopo de prontidão, que identifica a célula na qual cada atributo está contido.

3a. Crie um conjunto de atributos que reflita os atributos do nosso aplicativo Simple-Service.

```
aws route53-recovery-readiness --region us-west-2 create-resource-set \
    --resource-set-name ImportantInformationTables \
    --resource-set-type AWS::DynamoDB::Table \
    --resources
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
west-cell"
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
east-cell"
```

```
{
    "ResourceSetArn": "arn:aws:route53-recovery-readiness::111122223333:resource-set/
sample-resource-set",
    "ResourceSetName": "ImportantInformationTables",
    "Resources": [
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
        }
    ],
    "Tags": {}
}
```

3b. (Opcional) Você pode verificar o que está incluído no conjunto de atributos chamando a API `list-resource-sets`. Isso lista todos os conjuntos de atributos de uma conta da AWS. Aqui você pode ver que temos apenas um conjunto de atributos que criamos acima.

```
aws route53-recovery-readiness --region us-west-2 list-resource-sets
```

```
{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
            ],
            "Tags": {}
        }
    ]
}{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
```

```
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-
readiness::&ExampleAWSAccountNo1;:cell/east-cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
            ],
            "Tags": {}
        }
    ]
}
```

Agora, criamos as células, o grupo de recuperação e o conjunto de atributos para modelar o aplicativo Simple-Service no Route 53 ARC. Em seguida, configuraremos verificações de prontidão para monitorar a prontidão dos atributos para o failover.

## 4. Criar uma verificação de prontidão

Uma verificação de prontidão aplica um conjunto de regras a cada atributo no conjunto de atributos anexado à verificação. As regras são específicas para cada tipo de atributo. Ou seja, existem regras diferentes para `AWS::DynamoDB::Table`, `AWS::EC2::Instance` e assim por diante. As regras verificam uma variedade de dimensões de um atributo, incluindo configuração, capacidade e limites (quando disponíveis e aplicáveis), e configurações de roteamento.

> **Note**
>
> Para ver as regras que são aplicadas a um atributo em uma verificação de prontidão, você pode usar a API `get-readiness-check-resource-status`, conforme descrito na Etapa 5. Para ver uma lista de todas as regras de prontidão no Route 53 ARC, use `list-rules` ou consulte Descrições das regras de prontidão no Route 53 ARC. O Route 53 ARC tem um conjunto específico de regras que ele executa para cada tipo de atributo. Elas não são personalizáveis no momento.

4a. Crie uma verificação de prontidão para o conjunto de atributos, ImportantInformationTables.

```
aws route53-recovery-readiness --region us-west-2 create-readiness-check \
    --readiness-check-name ImportantInformationTableCheck --resource-set-name
 ImportantInformationTables
```

```
{
    "ReadinessCheckArn": "arn:aws:route53-recovery-readiness::111122223333:readiness-
check/ImportantInformationTableCheck",
    "ReadinessCheckName": "ImportantInformationTableCheck",
    "ResourceSet": "ImportantInformationTables",
    "Tags": {}
}
```

4b. (Opcional) Para verificar se a verificação de prontidão foi criada com êxito, execute a API `list-readiness-checks`. Essa API mostra todas as verificações de prontidão em uma conta.

```
aws route53-recovery-readiness --region us-west-2 list-readiness-checks
```

```
{
    "ReadinessChecks": [
        {
            "ReadinessCheckArn": "arn:aws:route53-recovery-
readiness::111122223333:readiness-check/ImportantInformationTableCheck",
            "ReadinessCheckName": "ImportantInformationTableCheck",
            "ResourceSet": "ImportantInformationTables",
            "Tags": {}
        }
    ]
}
```

## 5. Monitorar verificações de prontidão

Agora que modelamos o aplicativo e adicionamos uma verificação de prontidão, estamos prontos para monitorar os atributos. Você pode modelar a prontidão do seu aplicativo em quatro níveis: o nível de verificação de prontidão (um grupo de atributos), o nível de atributo individual, o nível da célula (todos os atributos em uma zona ou região de disponibilidade) e o nível do grupo de recuperação (o aplicativo como um todo). Os comandos para obter cada um desses tipos de status de prontidão são fornecidos abaixo.

5a. Ver o status da sua verificação de prontidão.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status\
    --readiness-check-name ImportantInformationTableCheck
```

```
{
    "Readiness": "READY",
    "Resources": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast2"
    ]
}
```

5b. Veja o status detalhado de prontidão de um único atributo em uma verificação de prontidão, incluindo o status de cada regra verificada.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-resource-status \
    --readiness-check-name ImportantInformationTableCheck \
    --resource-identifier "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
```

```
{"Readiness": "READY",
    "Rules": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoTableStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
```

```
            "RuleId": "DynamoCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsConfig"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoReplicationLatency"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoAutoScalingConfiguration"
        },
```

```
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoLimits"
        }
    ]
}
```

5c. Ver a prontidão geral de uma célula.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary \
    --cell-name west-cell
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

5d. Por fim, veja a prontidão de nível superior do seu aplicativo, no nível do grupo de recuperação.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary
 \
    --recovery-group-name simple-service-recovery-group
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

# Comece com o controle de roteamento usando a AWS CLI

Com o controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53, você pode acionar failovers de tráfego entre cópias ou réplicas redundantes de aplicativos que estão sendo executadas em Regiões da AWS ou zonas de disponibilidade distintas.

Você pode organizar os controles de roteamento em grupos chamados painéis de controle que são provisionados em um cluster. Um cluster do Route 53 ARC é um conjunto regional de endpoints implantado globalmente. Os endpoints de cluster fornecem uma API altamente disponível que você pode usar para definir e recuperar estados de controle de roteamento. Para obter mais informações sobre os componentes do atributo de controle de roteamento, consulte Componentes do controle de roteamento .

Nossa primeira etapa é criar um cluster. Um cluster do Route 53 ARC é um conjunto de cinco endpoints regionais que são implantados em uma distribuição global. A infraestrutura do Route 53 ARC suporta esses endpoints para trabalhar em coordenação para fornecer uma garantia de alta disponibilidade e consistência sequencial das operações de failover.

> **Note**
>
> O Route 53 ARC é um serviço global que oferece suporte a endpoints em várias Regiões da AWS, mas você deve especificar a região Oeste dos EUA (Oregon), ou seja, especificar o parâmetro `--region us-west-2`, na maioria dos comandos da CLI do Route 53 ARC. Por exemplo, para criar atributos como grupos de recuperação, verificações de prontidão ou clusters.
>
> Quando você cria um cluster, o Route 53 ARC fornece um conjunto de endpoints regionais. Para obter ou atualizar os estados de controle de roteamento, você deve especificar o endpoint regional (a Região da AWS e a URL do endpoint) em seu comando na CLI.

Para obter informações sobre como usar a AWS CLI, consulte a Referência de comandos da AWS CLI. Para conferir uma lista das ações de API de configuração de controle de recuperação e links para mais informações, consulte Operações de API de configuração do controle de recuperação.

## 1. Criar um cluster

1a. Crie um cluster.

```
aws route53-recovery-control-config --region us-west-2 create-cluster --cluster-name
 NewCluster
```

```
{
    "Cluster": {
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "Name": "NewCluster",
        "Status": "PENDING"
    }
}
```

Quando você cria pela primeira vez um atributo do Route 53 ARC, ele fica com o status de `PENDING` enquanto o cluster estiver sendo criado. Você pode verificar o progresso chamando `describe-cluster`.

1b. Descrever um cluster

```
aws route53-recovery-control-config --region us-west-2 \
    describe-cluster --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
```

```
{
    "Cluster":{
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "ClusterEndpoints":[
            {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
            {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
            {"Endpoint": "https://host-cccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
            {"Endpoint": "https://host-dddddd.us-west-2.example.com", "Region":"us-
west-2"},
            {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
        ]
        "Name": "NewCluster",
        "Status": "DEPLOYED"
    }
```

```
}
```

Quando o status é DEPLOYED, o Route 53 ARC criou com sucesso o cluster com o conjunto de endpoints com os quais você pode interagir. Você pode listar todos os seus clusters chamando `list-clusters`.

1c. Listar seus clusters.

```
aws route53-recovery-control-config --region us-west-2 list-clusters
```

```
{
    "Clusters": [
        {
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/1234abcd-abcd-1234-abcd-1234abcdefgh",
            "ClusterEndpoints":[
                {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
                {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
                {"Endpoint": "https://host-cccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
                {"Endpoint": "https://host-dddddd.us-west-2.example.com", "Region":"us-
west-2"},
                {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
            ],
            "Name": "AnotherCluster",
            "Status": "DEPLOYED"
        },
        {
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "ClusterEndpoints": [
                {"Endpoint": "https://host-ffffff.us-east-1.example.com", "Region":"us-
east-1"},
                {"Endpoint": "https://host-gggggg.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
                {"Endpoint": "https://host-hhhhhh.eu-west-1.example.com", "Region":"eu-
west-1"},
                {"Endpoint": "https://host-iiiiii.us-west-2.example.com", "Region":"us-
west-2"},
```

```
                {"Endpoint": "https://host-jjjjjj.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
            ],
            "Name": "NewCluster",
            "Status": "DEPLOYED"
        }
    ]
}
```

## 2. Criar um novo painel de controle.

Um painel de controle é um agrupamento lógico para organizar seus controles de roteamento do Route 53 ARC. Quando você cria um cluster, o Route 53 ARC fornece automaticamente um painel de controle para você chamado `DefaultControlPanel`. Você pode usar esse painel de controle imediatamente.

Um painel de controle só pode existir em um cluster. Se quiser mover um painel de controle para outro cluster, você deve excluí-lo e criá-lo no segundo cluster. Você pode ver todos os painéis de controle da sua conta chamando `list-control-panels`. Para ver apenas os painéis de controle em um cluster específico, adicione o campo `--cluster-arn`.

2a. Listar os painéis de controle.

```
aws route53-recovery-control-config --region us-west-2 \
    list-control-panels --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/eba23304-1a51-4674-ae32-b4cf06070bdd
```

```
{
    "ControlPanels": [
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/1234567dddddd1234567dddddd1234567",
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "DefaultControlPanel": true,
            "Name": "DefaultControlPanel",
            "RoutingControlCount": 0,
            "Status": "DEPLOYED"
        }
    ]
}
```

Opcionalmente, crie seu próprio painel de controle chamando `create-control-panel`.

2b. Cria um novo painel de controle.

```
aws route53-recovery-control-config --region us-west-2 create-control-panel \
        --control-panel-name NewControlPanel2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": false,
        "Name": "NewControlPanel2",
        "RoutingControlCount": 0,
        "Status": "PENDING"
    }
}
```

Quando você cria pela primeira vez um atributo do Route 53 ARC, ele tem o status de `PENDING` enquanto está sendo criado. Você pode verificar o progresso chamando `describe-control-panel`.

2c. Descrever um painel de controle.

```
aws route53-recovery-control-config --region us-west-2 describe-control-panel \
    --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": true,
        "Name": "DefaultControlPanel",
        "RoutingControlCount": 0,
```

```
        "Status": "DEPLOYED"
    }
}
```

## 3. Criar um controle de roteamento

Agora que você configurou o cluster e examinou os painéis de controle, pode começar a criar controles de roteamento. Ao criar um controle de roteamento, deverá especificar pelo menos o Nome do atributo da Amazon (ARN) do cluster em que deseja que o controle de roteamento esteja. Você também pode especificar o ARN de um painel de controle para o controle de roteamento. Especifique o cluster em que o painel de controle está localizado.

Se você não especificar um painel de controle, seu controle de roteamento será adicionado ao painel criado automaticamente, `DefaultControlPanel`.

Crie um controle de roteamento chamando `create-routing-control`.

3a. Criar um controle de roteamento.

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
    --routing-control-name NewRc1 \
    --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "RoutingControl": {
        "ControlPanelArn": " arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "PENDING"
    }
}
```

Os controles de roteamento seguem o mesmo padrão de criação de outros atributos do Route 53 ARC, então você pode acompanhar o progresso deles chamando uma operação de descrição.

3b. Descrever o controle de roteamento.

```
aws route53-recovery-control-config --region us-west-2 describe-routing-control \
       --routing-control-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "RoutingControl": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "DEPLOYED"
    }
}
```

Você pode listar os controles de roteamento em um painel de controle chamando `list-routing-controls`. O ARN do painel de controle é obrigatório.

3c. Listar os controles de roteamento.

```
aws route53-recovery-control-config --region us-west-2 list-routing-controls \
        --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "RoutingControls": [
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc1",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
            "Status": "DEPLOYED"
        },
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc2",
```

```
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
            "Status": "DEPLOYED"
        }
    ]
}
```

No exemplo a seguir, em que trabalhamos com estados de controle de roteamento, presumimos que você tenha os dois controles de roteamento listados nesta seção (Rc1 e Rc2). Neste exemplo, cada controle de roteamento representa uma zona de disponibilidade na qual seu aplicativo está implantado.

## 4. Criar uma regra de segurança

Ao trabalhar com vários controles de roteamento ao mesmo tempo, você pode decidir que deseja implementar algumas proteções ao ativá-los e desativá-los, para evitar consequências não intencionais, como desativar os dois controles de roteamento e interromper todo o fluxo de tráfego. Para criar essas proteções, crie regras de segurança do Route 53 ARC.

Existem dois tipos de regras de segurança: regras de afirmação e regras de isolamento. Para saber mais sobre as regras de segurança, consulte Criação de regras de segurança no Route 53 ARC .

A chamada a seguir fornece um exemplo de criação de uma regra de afirmação que garante que pelo menos um dos dois controles de roteamento seja definido como 0n a qualquer momento. Para criar a regra, você executa `create-safety-rule` com o parâmetro `assertion-rule`.

Para obter informações detalhadas sobre a operação da API da regra de afirmação, consulte Regra de afirmação no Guia de referência da API de controle de roteamento para o Controlador de recuperação de aplicações do Amazon Route 53.

4a. Criar uma regra de afirmação.

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --assertion-rule '{"Name": "TestAssertionRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "AssertedControls":
        ["arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
```

```
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
        "RuleConfig": {"Threshold": 1, "Type": "ATLEAST", "Inverted": false}}'
```

```
{
    "Rule": {
        "ASSERTION": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/333333444444",
            "AssertedControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestAssertionRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 1,
                "Type": "ATLEAST"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

A chamada a seguir fornece um exemplo de como criar uma regra de isolamento que fornece uma chave geral “liga/desliga” ou “controle” para um conjunto de controles de roteamento de destino em um painel. Isso permite que você proíba a atualização dos controles de roteamento de destino para que, por exemplo, a automação não possa fazer atualizações não autorizadas. Neste exemplo, a chave de controle é um controle de roteamento especificado pelo parâmetro `GatingControls` e os dois controles de roteamento que são controlados ou isolados são especificados pelo parâmetro `TargetControls`.

> **Note**
>
> Antes de criar a regra de isolamento, você deve criar o controle de roteamento de isolamento, que não inclui registros de failover de DNS, e os controles de roteamento de destino, que você configura com registros de failover de DNS.

Para criar a regra, execute `create-safety-rule` com o parâmetro `gating-rule`.

Para obter informações detalhadas sobre a operação da API da regra de afirmação, consulte Regra de isolamento no Guia de referência da API de controle de roteamento para o Controlador de recuperação de aplicações do Amazon Route 53.

4b. Criar uma regra de isolamento.

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --gating-rule '{"Name": "TestGatingRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "GatingControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
def123def123def"]
        "TargetControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
ghi456ghi456ghi",
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"],
        "RuleConfig": {"Threshold": 0, "Type": "OR", "Inverted": false}}'
```

```
{
    "Rule": {
        "GATING": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/444444444444",
            "GatingControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
            ],
            "TargetControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"
```

```
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"
            ],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestGatingRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 0,
                "Type": "OR"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

Assim como acontece com outros atributos do Route 53 ARC, você pode descrever, listar ou excluir regras de segurança depois que elas se propagam para o plano de dados.

Depois de configurar uma ou mais regras de segurança, você pode continuar a interagir com o cluster para definir ou recuperar o estado dos controles de roteamento. Se uma operação `set-routing-control-state` violar uma regra criada, você receberá uma exceção semelhante à seguinte:

```
Cannot modify control state for [0123456bbbbbbb0123456bbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbb0123456333333444444
```

O primeiro identificador é o ARN do painel de controle concatenado com o ARN do controle de roteamento. O segundo identificador é o ARN do painel de controle concatenado com a regra de segurança ARN.

## 5. Criar verificações de integridade

Para usar controles de roteamento para fazer failover do tráfego, crie verificações de saúde no Amazon Route 53 e associe-as aos seus registros de DNS. Como exemplo, digamos que você tenha duas células, uma que você configurou como a célula primária do seu aplicativo e a outra que você configurou como secundária, para a qual realizar o failover.

Para configurar verificações de saúde para failover, você pode fazer o seguinte, por exemplo:

1. Usar a CLI do Route 53 ARC para criar um controle de roteamento para cada célula.
2. Usar a CLI do Route 53 para criar uma verificação de integridade do Route 53 ARC no Route 53 para cada controle de roteamento.
3. Usar a CLI do Route 53 para criar dois registros DNS de failover no Route 53 e associar uma verificação de integridade a cada um.

5a. Criar um controle de roteamento para cada célula.

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell1 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

5b. Criar uma verificação de integridade para cada controle de roteamento.

> **Note**
>
> Crie verificações de saúde do Route 53 ARC usando a CLI do Amazon Route 53.

```
aws route53 create-health-check --caller-reference RoutingControlCell1 \
        --health-check-config \
        Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-fffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell1",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
```

```
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

```
aws route53 create-health-check --caller-reference RoutingControlCell2 \
    --health-check-config \
    Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell2",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

5c. Crie dois registros DNS de failover e associe uma verificação de integridade a cada um.

Crie registros DNS de failover no Route 53 usando a CLI do Route 53. Para criar os registros, siga as instruções na Referência de comandos da AWS CLI do Amazon Route 53 para o comando change-resource-record-sets. Nos registros, especifique o valor de DNS para cada célula junto com o valor de `HealthCheckID` correspondente que o Route 53 criou para a verificação de integridade (consulte 6b).

Para a célula primária:

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "primary",
    "Failover": "PRIMARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell1.yourdomain.com"
        }
    ],
    "HealthCheckId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

Para a célula secundária:

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "secondary",
    "Failover": "SECONDARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell2.yourdomain.com"
        }
    ],
    "HealthCheckId": "yyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy"
}
```

Agora, para fazer o failover da célula primária para a célula secundária, você pode seguir o exemplo da CLI na etapa 4b para atualizar o estado de `RoutingControlCell1` para `OFF` e de `RoutingControlCell2` para `ON`.

# Listar e atualizar os controles e estados de roteamento com a AWS CLI

Depois de criar seus atributos do Controlador de recuperação de aplicações do Amazon Route 53 (cluster, controles de roteamento e painéis de controle) você pode interagir com o cluster para listar e atualizar os estados do controle de roteamento.

Para cada cluster que você criar, o Route 53 ARC fornece um conjunto de endpoints de cluster, um em cada cinco Regiões da AWS. Você deve especificar um desses endpoints regionais (a Região da AWS e a URL do endpoint) ao fazer chamadas para o cluster para recuperar ou definir estados de controle de roteamento como `On` ou `Off`. Além do endpoint regional, você também deve especificar o `--region` endpoint regional ao usar a AWS CLI com o Route 53 ARC, conforme mostrado nos exemplos desta seção.

Você pode usar qualquer um dos endpoints do cluster regional. Recomendamos que seus sistemas estejam preparados para tentar novamente com cada um dos endpoints disponíveis. Para exemplos de código que ilustram como testar endpoints de cluster em sequência, consulte Ações para o Application Recovery Controller usando AWS SDKs.

Para obter informações sobre como usar a AWS CLI, consulte a Referência de comandos da AWS CLI. Para conferir uma lista das ações de API de controle de roteamento e links para mais informações, consulte Operações de API do plano de dados do cluster de recuperação (controle de roteamento).

> **Important**
>
> Embora você possa atualizar um estado de controle de roteamento no console do Amazon Route 53, recomendamos que você atualize os estados de controle de roteamento usando a AWS CLI ou um AWS SDK. O Route 53 ARC oferece extrema confiabilidade com o plano de dados de controle de roteamento do Route 53 ARC para redirecionar o tráfego e realizar o failover entre células. Para obter mais recomendações sobre o uso do Route 53 ARC para failover, consulte Práticas recomendadas para o Controlador de recuperação de aplicações do Amazon Route 53.

Quando você cria um controle de roteamento, o estado é definido como `Off`. Isso significa que o tráfego não é roteado para a célula de destino desse controle de roteamento. Você pode verificar o estado do controle de roteamento executando o comando `get-routing-control-state`.

Para determinar a região e o endpoint a serem especificados, execute o comando `describe-clusters` para visualizar o `ClusterEndpoints`. Cada `ClusterEndpoint` inclui uma região e um endpoint correspondente que você pode usar para obter ou atualizar os estados de controle de roteamento. Descrever cluster é uma operação de API de configuração de controle de recuperação. Recomendamos que você mantenha uma cópia local dos endpoints do cluster regional do Route 53 ARC, em marcadores ou codificada no código de automação que você usa para tentar novamente seus endpoints.

Você pode visualizar seus controles de roteamento e estados de controle de roteamento usando os endpoints altamente confiáveis do plano de dados do Route 53 ARC.

1. Liste os controles de roteamento para um painel de controle específico. Se você não especificar um painel de controle, o `list-routing-controls` retornará todos os controles de roteamento no cluster.

```
aws route53-recovery-cluster list-routing-controls --control-panel-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{
    "RoutingControls": [{
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlName": "RCOne",
        "RoutingControlState": "On"
    },
    {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
zzzzxxxxyyyy123456",
        "RoutingControlName": "RCTwo",
        "RoutingControlState": "Off"
```

```
    }
]
```

2. Obter um estado de controle de roteamento.

```
aws route53-recovery-cluster get-routing-control-state --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
    "RoutingControlName": "RCOne",
    "RoutingControlState": "On"
}
```

Para rotear o tráfego para o endpoint de destino controlado pelo controle de roteamento, atualize o estado do controle de roteamento para On. Atualize o estado do controle de roteamento executando o comando `update-routing-control-state`. Quando a solicitação for bem-sucedida, a resposta estará vazia.

2a. Atualizar um estado de controle de roteamento.

```
aws route53-recovery-cluster update-routing-control-state \
        --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --routing-control-state On \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

Você pode atualizar vários controles de roteamento ao mesmo tempo com uma chamada de API:`update-routing-control-states`. Quando a solicitação for bem-sucedida, a resposta estará vazia.

2b. Atualizar vários estados de controle de roteamento de uma só vez (atualizações em lote).

```
aws route53-recovery-cluster update-routing-control-states \
        --update-routing-control-state-entries \
        '[{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlState": "Off"}, \
        {"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
        "RoutingControlState": "On"}]' \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

# Comece com a mudança de zona usando a AWS CLI

A mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53 permite que você mova temporariamente o tráfego de seus balanceadores de carga para fora de uma zona de disponibilidade, para que seu aplicativo possa continuar operando normalmente com outras zonas de disponibilidade em uma Região da AWS. Atualmente, a mudança de zona oferece suporte a Network Load Balancers e Application Load Balancers com o balanceador de carga entre zonas desativado.

Vejamos um exemplo de como iniciar uma mudança de zona usando a AWS Command Line Interface. Você também pode usar a AWS CLI para atualizar uma mudança de zona, por exemplo, para definir uma nova expiração. Todas as mudanças de zona são temporárias e devem ser definidas inicialmente para expirar em três dias. No entanto, você pode atualizar uma mudança de zona posteriormente para definir uma nova expiração.

Para obter informações sobre como usar a AWS CLI, consulte a Referência de comandos da AWS CLI. Para conferir uma lista de ações de API de mudança de zona e links para mais informações, consulte Operações de API de mudança de zona.

## Iniciar mudança de zona

Você pode iniciar uma mudança de zona com a CLI usando o comando `start-zonal-shift`.

```
aws arc-zonal-shift start-zonal-shift \
```

```
      --resource-identifier="arn:aws:testservice::111122223333:ExampleALB123456890" \
      --away-from="usw2-az1" \
      --expires-in="5m" \
      --comment="Shifting traffic away from USW2-AZ1"
```

```
{
   "zonalShiftId": "2222222-3333-444-1111",
   "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
   "awayFrom": "usw2-az1",
   "expiryTime": 2022-11-14T01:40:42+00:00,
   "startTime": 2022-11-14T01:35:42+00:00,
   "status": "ACTIVE",
   "comment": "Shifting traffic away from USW2-AZ1"
}
```

## Obter atributos gerenciados

Você pode obter informações sobre um atributo gerenciado com a CLI usando o comando `get-managed-resource`.

```
aws arc-zonal-shift get-managed-resource \
   --resource-identifier="arn:aws:testservice::111122223333:ExampleALB123456890
```

```
{
    "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "name": "TestResource",
    "appliedWeights": {
        "usw2-az1": 1.0,
        "usw2-az2": 1.0,
        "usw2-az3": 1.0
    },
    "zonalShifts": []
}
```

## Listar atributos gerenciados

Você pode listar os atributos gerenciados em sua conta com a CLI usando o comando `list-managed-resources`.

```
aws arc-zonal-shift list-managed-resources
```

```
{
    "items": [
        {
            "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
            "name": "TestResource",
            "availabilityZones": [
                "usw2-az1",
                "usw2-az2",
                "usw2-az3"
            ]
        }
    ]
}
```

## Listar mudanças de zona

Você pode listar as mudanças de zona em sua conta com a CLI usando o comando `list-zonal-shifts`.

```
aws arc-zonal-shift list-zonal-shifts
```

```
{
    "items": [
        {
            "zonalShiftId": "2222222-3333-444-1111",
            "resourceIdentifier":
 "arn:aws:testservice::111122223333:ExampleALB123456890",
            "awayFrom": "usw2-az1",
            "expiryTime": 2022-11-15T09:10:42+00:00,
            "startTime": 2022-11-13T01:35:42+00:00,
            "status": "ACTIVE",
            "comment": "Shifting traffic away from USW2-AZ1"
        }
    ]
}
```

## Atualizar mudança de zona

Você pode atualizar uma mudança de zona com a CLI usando o `update-zonal-shift`.

```
aws arc-zonal-shift update-zonal-shift \
```

```
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890" \
   --expires-in="1h" \
   --comment="Still shifting traffic away from USW2-AZ1"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2022-11-15T10:35:42+00:00,
    "startTime": 2022-11-15T09:35:42+00:00,
    "status": "ACTIVE",
    "comment": "Still shifting traffic away from USW2-AZ1"
}
```

## Cancelar mudança de zona

Você pode cancelar uma mudança de zona com a CLI usando o comando `cancel-zonal-shift`.

```
aws arc-zonal-shift cancel-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2022-11-15T10:35:42+00:00,
    "startTime": 2022-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Shifting traffic away from USW2-AZ1"
}
```

# Começar a usar a mudança automática de zona com a AWS CLI

A mudança automática de zona é um recurso do Controlador de Recuperação de Aplicações do Amazon Route 53. Com a mudança automática de zona, você autoriza a AWS a transferir o tráfego de recursos da aplicação para fora de uma zona de disponibilidade durante eventos, em seu nome, para ajudar a reduzir o tempo de recuperação. A mudança automática de zona inclui execuções práticas para ajudar você a garantir que as mudanças automáticas sejam seguras para a aplicação.

No momento, a mudança automática de zona oferece suporte a Network Load Balancers e Application Load Balancers com o balanceamento de carga entre zonas desativado.

Para obter mais informações, consulte Mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53.

Esta seção fornece os exemplos a seguir para ilustrar como começar e trabalhar com a mudança automática de zona:

- Crie uma configuração de execução prática para um recurso.
- Habilite e desabilite as mudanças automáticas para um recurso.
- Encerre uma execução prática em andamento, cancelando a mudança de zona iniciada pela execução prática.
- Encerre uma mudança automática em andamento, desabilitando a mudança automática de zona para um recurso.
- Edite uma configuração de execução prática de um recurso para alterar os alarmes especificados ou as datas ou janelas bloqueadas.
- Exclua uma configuração de execução prática para um recurso.

Para obter informações sobre como usar a AWS CLI, consulte a Referência de comandos da AWS CLI. Para conferir uma lista de ações de API de mudança automática de zona e links para mais informações, consulte Operações de API de mudança automática de zona.

## Criar uma configuração de execução prática

Antes de habilitar a mudança automática de zona para um recurso, é necessário criar uma configuração de execução prática para o recurso a fim de escolher opções para as execuções práticas necessárias. Crie uma configuração de execução prática para um recurso com a CLI usando o comando `create-practice-run-configuration`.

Observe o seguinte ao criar uma configuração de execução prática para um recurso:

- O único tipo de alarme compatível por enquanto é `CLOUDWATCH`.
- Você deve usar alarmes que estejam na mesma Região da AWS de implantação do recurso.
- É necessário especificar um alarme de resultado. Especificar um alarme de bloqueio é opcional.
- Especificar datas ou janelas bloqueadas é opcional.

Crie uma configuração de execução prática com a CLI usando o comando `create-practice-run-configuration`.

Por exemplo, para criar uma configuração de execução prática para um recurso, use um comando semelhante ao seguinte:

```
aws arc-zonal-shift create-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --outcome-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
MyAppHealthAlarm \
      --blocking-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
BlockWhenALARM \
      --blocked-dates 2023-12-01 --blocked-windows Mon:10:00-Mon:10:30
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                  {
              "type": "CLOUDWATCH",
              "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
       "blockedWindows": [
           "Mon:10:00-Mon:10:30"
       ],
       "blockedDates": [
           "2023-12-01"
       ]
```

```
}
```

## Habilitar ou desabilitar mudanças automáticas

Habilite ou desabilite as mudanças automáticas para um recurso atualizando o status da mudança automática de zona com a CLI. Para alterar o status da mudança automática de zona, use o comando `update-zonal-autoshift-configuration`.

Por exemplo, para habilitar as mudanças automáticas para um recurso, use um comando semelhante ao seguinte:

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="ENABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "ENABLED"
}
```

## Cancelar uma mudança automática em andamento

Para cancelar uma mudança automática em andamento para um recurso, desabilite a mudança automática de zona. Esse é o mesmo comando que você usa para desabilitar a mudança automática de zona de forma geral, portanto, quando você desabilitar a mudança automática de zona para cancelar uma mudança automática em andamento, o recurso também não será afetado por futuras mudanças automáticas. Você pode atualizar a mudança automática de zona para habilitá-la novamente a qualquer momento.

Observe que você pode desabilitar a mudança automática de zona para um recurso sem excluir a configuração de execução prática do recurso.

Para cancelar uma mudança automática com a CLI, desabilite a mudança automática de zona usando o comando `update-zonal-autoshift-configuration`. Por exemplo, para encerrar uma mudança automática para um recurso, use um comando semelhante ao seguinte:

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
```

```
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

## Cancelar uma execução prática em andamento

Você pode cancelar uma execução prática em andamento com a CLI, cancelando a mudança de zona que a execução prática iniciou para o recurso. Para cancelar uma execução prática, use o comando `cancel-zonal-shift`.

Por exemplo, para cancelar uma execução prática para um recurso, use um comando semelhante ao seguinte:

```
aws arc-zonal-shift cancel-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2024-11-15T10:35:42+00:00,
    "startTime": 2024-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Practice Run Started"
}
```

## Editar uma configuração de execução prática

Você pode editar uma configuração de execução prática para um recurso com a CLI a fim de atualizar diferentes opções de configuração, como alterar os alarmes para execuções práticas ou atualizar as datas ou janelas bloqueadas, quando o Route 53 ARC não inicia as execuções práticas. Para editar uma configuração de execução prática, use o comando `update-practice-run-configuration`.

Observe o seguinte ao editar uma configuração de execução prática para um recurso:

- O único tipo de alarme compatível por enquanto é `CLOUDWATCH`.
- Você deve usar alarmes que estejam na mesma Região da AWS de implantação do recurso.
- É necessário especificar um alarme de resultado. Especificar um alarme de bloqueio é opcional.
- Especificar datas ou janelas bloqueadas é opcional.
- As datas ou janelas bloqueadas que você especificar substituirão quaisquer valores existentes.

Por exemplo, para editar uma configuração de execução prática para um recurso a fim de especificar uma nova data bloqueada, use um comando semelhante ao seguinte:

```
aws arc-zonal-shift update-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --blocked-dates 2024-03-01
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                   {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
       "blockedWindows": [
           "Mon:10:00-Mon:10:30"
       ],
       "blockedDates": [
           "2024-03-01"
```

```
        ]
}
```

## Excluir uma configuração de execução prática

Você pode excluir uma configuração de execução prática para um recurso, mas antes deve desabilitar a mudança automática de zona para o recurso. É necessário que um recurso tenha uma configuração de execução prática para habilitar a mudança automática de zona. As execuções práticas regulares ajudam você a garantir que a aplicação possa ser executada normalmente sem uma zona de disponibilidade.

Para excluir uma configuração de execução prática usando a CLI, primeiro desabilite a mudança automática de zona, se necessário, usando o comando `update-zonal-autoshift`. Depois, para excluir a configuração da execução prática, use o comando `delete-practice-run-configuration`.

Primeiro, desabilite a mudança automática de zona para o recurso usando um comando como o seguinte:

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Depois, exclua a configuração da execução prática usando um comando como o seguinte:

```
aws arc-zonal-shift delete-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890"
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "TestResource",
```

```
    "zonalAutoshiftStatus": "DISABLED"
}
```

# Práticas recomendadas para o Controlador de recuperação de aplicações do Amazon Route 53

Para minimizar as interrupções e ajudar a garantir a continuidade operacional, siga as melhores práticas para planejar e executar a recuperação de desastres com o Controlador de recuperação de aplicações do Amazon Route 53. Revise as diretrizes deste capítulo para saber mais.

Tópicos



## Práticas recomendadas para recuperação no Route 53 ARC

Recomendamos as seguintes práticas para recuperação e preparação para o failover no Controlador de recuperação de aplicações do Amazon Route 53.

Mantenha as credenciais da AWS personalizadas e de longa duração seguras e sempre acessíveis

Em um cenário de recuperação de desastres (DR), reduza ao mínimo as dependências do sistema usando uma abordagem simples para acessar a AWS e executar tarefas de recuperação. Crie credenciais de longa duração do IAM especificamente para tarefas de DR e mantenha as credenciais com segurança em um cofre físico local ou em um cofre virtual, para acessar quando necessário. Com o IAM, é possível gerenciar de forma centralizada usuários, credenciais de segurança como chaves de acesso e permissões que controlam quais recursos da AWS os usuários podem acessar. Para tarefas que não sejam de DR, recomendamos que você continue usando o acesso federado, usando serviços da AWS como o AWS Single Sign-On.

Para realizar tarefas de failover no Route 53 ARC com a API do plano de dados do cluster de recuperação, você pode anexar uma política de IAM do Route 53 ARC ao seu usuário. Para saber mais, consulte Exemplos de políticas baseadas em identidade do Controlador de recuperação de aplicações do Amazon Route 53.

Escolha valores de Time to live (TTL) mais baixos para registros de DNS envolvidos no failover

Para registros DNS que talvez você precise alterar como parte do mecanismo de failover, especialmente registros com verificação de integridade, é apropriado usar valores de TTL mais baixos. Definir um TTL de 60 ou 120 segundos é comum para esse cenário.

A configuração DNS TTL informa aos resolvedores de DNS por quanto tempo armazenar um registro em cache antes de solicitar um novo. 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 consultá-lo com mais frequência.

Para obter mais informações, consulte Escolher valores de TTL para registros DNS em Práticas recomendadas para o DNS do Amazon Route 53.

# Práticas recomendadas para mudanças de zona no Route 53 ARC

Recomendamos seguir as práticas recomendadas para uso de mudanças de zona para recuperação multi-AZ no Route 53 ARC. As mudanças de zona normalmente removem a capacidade de um aplicativo ativo, por isso é importante ter cuidado ao usá-las na produção.

Planejamento de capacidade e pré-escalabilidade

Verifique se você planejou e pré-escalou ou pode escalar automaticamente a capacidade suficiente para acomodar a carga extra imposta às zonas de disponibilidade ao iniciar uma mudança de zona. Com uma arquitetura orientada à recuperação, uma recomendação típica é pré-escalar a capacidade computacional para incluir espaço suficiente para atender ao pico de tráfego quando uma de suas (normalmente) três réplicas estiver off-line.

Quando você inicia uma mudança de zona para um único recurso de balanceador de carga, por exemplo, a capacidade de uma zona de disponibilidade é temporariamente removida de trás do balanceador de carga. Dependendo das mudanças de zona que você inicia e de como seus balanceadores de carga estão configurados, você deve se certificar de ter planejado cuidadosamente o gerenciamento do aumento de carga nas demais zonas de disponibilidade.

Testar o início das mudanças de zona com antecedência

Teste regularmente a remoção do tráfego das zonas de disponibilidade para seu aplicativo iniciando mudanças de zona. Planeje e execute mudanças de zona iniciais, preferencialmente

em ambientes de teste e produção, como parte dos testes regulares de failover para recuperar seus aplicativos em caso de desastre. Testes regulares são uma parte essencial para garantir que você esteja pronto e tenha a confiança necessária para mitigar problemas quando ocorrer um evento operacional.

Garanta que todas as zonas de disponibilidade estejam saudáveis e recebam tráfego

As mudanças de zona funcionam marcando um recurso, ou seja, uma réplica de aplicativo, como não íntegro em uma zona de disponibilidade. Isso significa que é fundamental garantir que os destinos nos balanceadores de carga de seus aplicativos geralmente estejam íntegros e recebam tráfego ativamente nas zonas de disponibilidade de uma região. Recomendamos que você tenha painéis para monitorar isso, incluindo, por exemplo, métricas do Elastic Load Balancing para alvos não íntegros e bytes processados por zona de disponibilidade.

Considere monitorar a integridade de seus recursos em uma segunda região adjacente. A vantagem dessa abordagem é que ela pode ser mais representativa da experiência de seus usuários finais. Ela também reduz o risco de seu aplicativo e seu monitoramento serem afetados pelo mesmo desastre ao mesmo tempo ("destino compartilhado").

Use operações de API de plano de dados para recuperação de desastres

Para iniciar uma mudança de zona quando você precisa recuperar um aplicativo rapidamente, com poucas dependências, recomendamos usar a AWS Command Line Interface ou API com ações de mudança de zona, com credenciais pré-armazenadas, se possível. Você também pode iniciar mudanças de zona no AWS Management Console, para facilitar o uso. Mas quando uma recuperação rápida e confiável é essencial, as operações do plano de dados são a melhor escolha. Para mais informações, consulte Guia de referência da API de mudança de zona.

Mova o tráfego com uma mudança de zona apenas temporariamente

Uma mudança de zona afasta o tráfego de uma zona de disponibilidade temporariamente para mitigar uma deficiência. Você deve restaurar o recurso para manutenção do aplicativo assim que tiver tomado medidas para corrigir um problema. Isso garante que seu aplicativo geral seja restaurado ao estado original, totalmente redundante e resiliente.

# Práticas recomendadas para mudanças automáticas de zona no Route 53 ARC

Recomendamos as práticas recomendadas a seguir para habilitar a mudança automática de zona para recuperação multi-AZ no Route 53 ARC. As execuções práticas e mudanças automáticas com

mudança de zona removem capacidade de uma aplicação ativa, por isso é importante ter cuidado ao usar ou habilitar esses recursos na produção.

Planejamento de capacidade e pré-escalabilidade

Ao planejar a configuração da mudança automática de zona para um recurso, ajuste a escala de capacidade da aplicação previamente. Depois, inicie uma ou mais mudanças de zona para o recurso, a fim de transferir o tráfego para fora de uma zona de disponibilidade e verifique se a aplicação continua operando normalmente com a perda de uma zona de disponibilidade. Quando você configura a mudança automática de zona, o Route 53 ARC inicia regularmente mudanças de zona de execução prática para o recurso, a fim de ajudar você a confirmar que pode operar a aplicação normalmente com a perda de uma zona de disponibilidade.

Criar alarmes direcionados do CloudWatch para execuções práticas

Para execuções práticas em mudança automática de zona, especifique um alarme do CloudWatch para monitorar a integridade da aplicação quando o tráfego é transferido para fora de uma zona de disponibilidade durante uma execução prática. Configure os limites para o alarme do CloudWatch para que uma execução prática seja interrompida antes que a performance da aplicação diminua, de modo que os clientes possam continuar usando a aplicação normalmente. Para obter mais informações, consulte a seção Alarmes que você especifica para execuções práticas em Considerações ao configurar a mudança automática de zona.

# Práticas recomendadas para verificações de prontidão e controles de roteamento no Route 53 ARC

Recomendamos as seguintes melhores práticas para prontidão de recuperação e preparação para failover quando você configura e usa o Route 53 ARC com verificações de prontidão e controle de roteamento, por exemplo, para failover regional.

Marque ou codifique rigidamente seus cinco endpoints de cluster regionais e ARNs de controle de roteamento

Recomendamos que você mantenha uma cópia local dos endpoints do cluster regional do Route 53 ARC, em marcadores ou salva no código de automação que você usa para testar novamente seus endpoints. Durante um evento de falha, talvez você não consiga acessar algumas operações de API, incluindo operações de API do Route 53 ARC que não estão

hospedadas no cluster de plano de dados extremamente confiável. Você pode listar os endpoints dos seus clusters do Route 53 ARC usando a operação da API Descrever Cluster.

Escolha um de seus endpoints aleatoriamente para atualizar seus estados de controle de roteamento

Recomendamos que, quando você precisar fazer o failover, atualize (e recupere) os estados de controle de roteamento usando um endpoint aleatório de seus cinco endpoints de cluster regionais. Se esse endpoint falhar, tente novamente cada um dos outros endpoints regionais. Para obter informações sobre como usar exemplos de código com o AWS SDK, incluindo exemplos para testar endpoints de cluster, consulte Exemplos de código para o Application Recovery Controller usando AWS SDKs.

Use a API de plano de dados extremamente confiável para listar e atualizar os estados de controle de roteamento, não o console

Usando a API de plano de dados do Route 53 ARC, visualize seus controles e estados de roteamento com a operação Listar controles de roteamento e atualize os estados de controle de roteamento para redirecionar o tráfego para failover com a operação Atualizar controle de estado de saída. Você pode usar a AWS CLI como nesses exemplos ou o código que você escrever usando um dos AWS SDKs. O Route 53 ARC oferece extrema confiabilidade com a API no plano de dados para failover do tráfego. Recomendamos usar a API em vez de alterar os estados de controle de roteamento no AWS Management Console.

Conecte-se a um de seus endpoints de cluster regionais para o Route 53 ARC para usar a API do plano de dados. Se o endpoint não estiver disponível, tente se conectar a outro endpoint do cluster.

Se uma regra de segurança bloquear uma atualização do estado do controle de roteamento, você poderá ignorá-la para fazer a atualização e fazer o failover do tráfego. Para obter mais informações, consulte Sobrepor regras de segurança para redirecionar o tráfego.

Testar o failover com o Route 53 ARC

Teste o failover regularmente com o controle de roteamento do Route 53 ARC, para fazer o failover de sua pilha de aplicativos primária para uma pilha de aplicativos secundária. É importante garantir que as estruturas do Route 53 ARC que você adicionou estejam alinhadas com os recursos corretos em sua pilha e que tudo funcione conforme o esperado. Você deve testar isso depois de configurar o Route 53 ARC para seu ambiente e continuar testando periodicamente, para que seu ambiente de failover esteja preparado, antes de enfrentar uma situação de falha na qual você precise que seu sistema secundário esteja pronto e funcionando rapidamente para evitar tempo de inatividade para seus usuários.

### Adicione notificações para alterações no status de prontidão

Defina uma regra no Amazon EventBridge para enviar uma notificação sempre que o status de uma verificação de prontidão mudar, por exemplo, de `READY` para `NOT READY`. Ao receber uma notificação, você pode investigar e resolver o problema para garantir que seu aplicativo e seus recursos estejam prontos para o failover quando você espera que estejam.

Você pode definir as regras do EventBridge para enviar notificações sobre várias alterações no status da verificação de prontidão, inclusive para seu grupo de recuperação (para seu aplicativo), para uma célula (como uma região da AWS) ou para uma verificação de prontidão para um conjunto de recursos.

Para obter mais informações, consulte Usando o Route 53 ARC com a Amazon EventBridge.

# Operações de API comuns para o Controlador de Recuperação de Aplicações do Amazon Route 53

Esta seção lista as operações de API comuns do Controlador de Recuperação de Aplicações do Amazon Route 53 que você pode usar, com links para a documentação relevante.

Para conferir exemplos de como usar muitas dessas operações com a AWS Command Line Interface, consulte Exemplos de uso das operações da API do Route 53 ARC com a AWS CLI.

Tópicos



## Operações de API de prontidão para recuperação (verificação de prontidão)

A tabela a seguir lista as operações do Route 53 ARC usadas na prontidão para recuperação (verificação de prontidão), com links para a documentação relevante.

Para conferir exemplos de como usar operações de API comuns de prontidão para recuperação com a AWS Command Line Interface, consulte Comece com a verificação de prontidão usando a AWS CLI.

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Criar uma célula | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Consulte Criar célula |

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Obter uma célula | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Veja Obter célula |
| Excluir uma célula | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Consulte Excluir célula |
| Atualizar uma célula | N/D | Consulte Atualizar célula |
| Listar células para uma conta | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Consulte Listar células |
| Criar um grupo de recuperação | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Consulte Criar grupo de recuperação |
| Obter um grupo de recuperação | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Consulte Obter grupo de recuperação |
| Atualizar um grupo de recuperação | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Consulte Atualizar grupo de recuperação |
| Excluir o grupo de recuperação | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Consulte Excluir grupo de recuperação |
| Listar grupos de recuperação | Consulte Criar, atualizar e excluir grupos de recuperação no Route 53 ARC | Veja Listar grupos de recuperação |

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Criar um conjunto de recursos. | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Criar conjunto de recursos |
| Obter um conjunto de recursos | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Obter um conjunto de recursos |
| Atualizar um conjunto de recursos | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Atualizar conjunto de recursos |
| Excluir um conjunto de recursos | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Excluir conjunto de recursos |
| Listar conjuntos de recursos | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Listar conjuntos de recursos |
| Criar uma verificação de prontidão | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Criar verificação de prontidão |
| Obter uma verificação de prontidão | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Obter verificação de prontidão |
| Atualizar uma verificação de prontidão | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Atualizar verificação de prontidão |
| Excluir uma verificação de prontidão | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Excluir verificação de prontidão |

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Listar verificações de prontidão | Consulte Criar e atualizar verificações de prontidão no Route 53 ARC | Consulte Listar verificações de prontidão |
| Listar regras de prontidão | Consulte Descrições das regras de prontidão no Route 53 ARC | Veja Listar regras |
| Obter o status de uma verificação de prontidão completa | Consulte Monitorar o status de prontidão no Route 53 ARC | Consulte Obter status de verificação de prontidão |
| Verificar o status de um recurso | Consulte Monitorar o status de prontidão no Route 53 ARC | Consulte Verificar o status de um recurso de verificação de prontidão |
| Verificar o status de uma célula | Consulte Monitorar o status de prontidão no Route 53 ARC | Consulte Verificar status da célula |
| Verificar o status de um grupo de recuperação | Consulte Monitorar o status de prontidão no Route 53 ARC | Consulte Verificar status do grupo de recuperação |

# Operações de API de configuração do controle de recuperação

A tabela a seguir lista as operações de API do Route 53 ARC usadas para a configuração do controle de recuperação, com links para a documentação relevante.

Para conferir exemplos de como usar operações de API comuns de configuração do controle de recuperação com a AWS Command Line Interface, consulte Comece com o controle de roteamento usando a AWS CLI.

| Ação | Usar o console do Route 53 ARC | Usar a API Route 53 ARC |
|---|---|---|
| Criar um cluster | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Criar cluster |
| Descrever um cluster | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Descrever cluster |
| Excluir um cluster | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Excluir cluster |
| Listar clusters para uma conta | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Listar clusters |
| Criar um controle de roteamento | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Criar um controle de roteamento |
| Descrever um controle de roteamento | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Descrever um controle de roteamento |
| Atualizar um controle de roteamento | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Atualizar um controle de roteamento |
| Excluir um controle de roteamento | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Excluir um controle de roteamento |
| Listar controles de roteamento | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Listar controles de roteamento |

| Ação | Usar o console do Route 53 ARC | Usar a API Route 53 ARC |
|---|---|---|
| Criar um novo painel de controle. | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Criar painel de controle |
| Descrever um painel de controle | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Descrever painel de controle |
| Atualizar um painel de controle | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Atualizar painel de controle |
| Excluir um painel de controle | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Excluir painel de controle |
| Listar painéis de controle | Consulte Criar componentes de controle de roteamento no Route 53 ARC | Consulte Listar painéis de controle |
| Criar uma regra de segurança | Consulte Criação de regras de segurança no Route 53 ARC | Consulte Criar regra de segurança |
| Descrever uma regra de segurança | Consulte Criação de regras de segurança no Route 53 ARC | Consulte Descrever regra de segurança |
| Atualizar uma regra de segurança | Consulte Criação de regras de segurança no Route 53 ARC | Consulte Atualizar regra de segurança |
| Excluir uma regra de segurança | Consulte Criação de regras de segurança no Route 53 ARC | Consulte Excluir regra de segurança |
| Listar regras de segurança | Consulte Criação de regras de segurança no Route 53 ARC | Consulte Listar regras de segurança |

| Ação | Usar o console do Route 53 ARC | Usar a API Route 53 ARC |
| --- | --- | --- |
| Listar as verificações de integridade do Route 53 associadas | Consulte Criar uma verificação de integridade do controle de roteamento no Route 53 ARC | Consulte Listar as verificações de integridade do Route 53 associadas |
| Listar as políticas de recursos de AWS RAM para compartil hamento de clusters | Consulte Suporte entre contas para clusters no Route 53 ARC | Consulte Obter política de recurso |

## Operações de API do plano de dados do cluster de recuperação (controle de roteamento)

A tabela a seguir lista as operações de API comuns do Route 53 ARC usadas para gerenciar o failover de tráfego com o plano de dados de controle de roteamento (cluster de recuperação), com links para a documentação relevante.

Para conferir exemplos de como usar operações de API de controle de roteamento com a AWS Command Line Interface, consulte Listar e atualizar os controles e estados de roteamento com a AWS CLI.

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Obter um estado de controle de roteamento | Consulte Obter e atualizar estados de controle de roteamento no AWS Management Console | Consulte Obter estado de controle de roteamento |
| Listar controles de roteamento | N/D | Consulte Listar controles |
| Atualizar um estado de controle de roteamento | Consulte Obter e atualizar estados de controle de roteamento no AWS Management Console | Consulte Atualizar estado de controle de roteamento |

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Atualizar vários estados de controle de roteamento | Consulte Obter e atualizar estados de controle de roteamento no AWS Management Console | Consulte Atualizar estados de controle de roteamento |

## Operações de API de mudança de zona

A tabela a seguir lista operações de API do Route 53 ARC usadas com a mudança de zona, que transfere o tráfego para fora de uma zona de disponibilidade para aplicações multi-AZ. A tabela também inclui links para a documentação relevante.

Para conferir exemplos de como usar operações de API comuns de mudança de zona com a AWS Command Line Interface, consulte Comece com a mudança de zona usando a AWS CLI.

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Iniciar uma mudança de zona | Consulte Iniciar uma mudança de zona | Consulte Iniciar mudança de zona |
| Atualizar um deslocamento de zona | Consulte Atualizar ou cancelar uma mudança de zona | Consulte Atualizar deslocamento de zona |
| Listar mudanças de zona | Consulte Mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53 | Consulte Listar mudanças de zona |
| Listar recursos gerenciados | Consulte Recursos compatíveis com mudança de zona e mudança automática de zona | Consulte Listar recursos gerenciados |

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Obter recursos gerenciados | Consulte Recursos compatíveis com mudança de zona e mudança automática de zona | Consulte Obter recursos gerenciados |
| Cancelar uma mudança de zona | Consulte Atualizar ou cancelar uma mudança de zona | Consulte Cancelar mudança de zona |

## Operações de API de mudança automática de zona

A tabela a seguir lista operações de API do Route 53 ARC usadas com a mudança automática de zona. Para conferir exemplos de como usar operações de API de mudança automática de zona com a AWS CLI, consulte .

Para conferir exemplos de como usar operações de API comuns de mudança automática de zona com a AWS Command Line Interface, consulte Começar a usar a mudança automática de zona com a AWS CLI.

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Criar uma configuração de execução prática | Consulte Habilitar ou desabilitar a mudança automática de zona | Consulte CreatePracticeRunConfiguration. |
| Excluir uma configuração de execução prática | Consulte Configurar, editar ou excluir uma configuração de execução prática | Consulte DeletePracticeRunConfiguration. |
| Listar mudanças automáticas | Consulte Mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53 | Consulte ListAutoshifts. |

| Ação | Usar o console do Route 53 ARC | Usar a API do Route 53 ARC |
| --- | --- | --- |
| Listar recursos para mudança automática de zona | Consulte Recursos compatíveis com mudança de zona e mudança automática de zona | Consulte Listar recursos gerenciados |
| Obter recursos para mudança automática de zona | Consulte Recursos compatíveis com mudança de zona e mudança automática de zona | Consulte Obter recursos gerenciados |
| Editar uma configuração de execução prática | Consulte Configurar, editar ou excluir uma configuração de execução prática | Consulte UpdatePracticeRunConfiguration. |
| Habilitar ou desabilitar a mudança automática de zona | Consulte Habilitar ou desabilitar a mudança automática de zona | Consulte UpdateZonalAutoshiftConfiguration. |

# Mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53

Este capítulo explica como usar a mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53 para recuperar seu aplicativo de forma confiável de um problema em uma zona de disponibilidade. Você pode iniciar uma mudança de zona para mover o tráfego de um recurso gerenciado do Elastic Load Balancing (ELB) em uma região da AWS para fora de uma zona de disponibilidade, por exemplo, porque uma implantação incorreta está causando problemas de latência ou porque a zona de disponibilidade está prejudicada.

Além de iniciar uma mudança de zona no Route 53 ARC, também é possível iniciar uma mudança de zona para um balanceador de carga no console do Elastic Load Balancing. Para saber mais sobre como iniciar uma mudança de zona com o Elastic Load Balancing, consulte Mudança de zona no Guia do usuário do Elastic Load Balancing.

Todas as mudanças de zona são temporárias. Você deve definir uma expiração inicial ao iniciar uma mudança de zona, de uma hora até três dias (72 horas). É possível atualizar as mudanças de zona ativas a qualquer momento para definir novas expirações. A nova expiração começa no momento em que você a define, e tem as mesmas restrições.

Tópicos



## Como funciona uma mudança de zona

Quando você inicia uma mudança de zona para um recurso de balanceador de carga, o Controlador de recuperação de aplicações do Amazon Route 53 solicita que o recurso afaste o tráfego da zona de disponibilidade que você especificou. Essa solicitação faz com que a verificação de integridade do balanceador de carga da zona de disponibilidade seja definida como não íntegra, de modo que falhe na verificação de integridade. Uma verificação de integridade, por sua vez, faz com que o Amazon Route 53 retire os endereços IP correspondentes do recurso do DNS, de forma que o tráfego seja

redirecionado da zona de disponibilidade. Em vez disso, novas conexões agora são roteadas para outras zonas de disponibilidade na região da AWS.

Ao iniciar uma mudança de zona, ela é criada no Route 53 ARC, mas devido às etapas do processo, talvez você não veja o tráfego sair da zona de disponibilidade imediatamente. Também pode levar um pouco de tempo para que as conexões existentes e em andamento na zona de disponibilidade sejam concluídas, dependendo do comportamento do cliente e da reutilização da conexão. Normalmente, isso demora apenas alguns minutos.

Quando uma mudança de zona iniciada pelo cliente expira ou você a cancela, o Route 53 ARC reverte o processo, solicitando que as verificações de integridade do Route 53 sejam definidas como íntegras novamente, para que os endereços IP das zonas originais sejam restaurados e a zona de disponibilidade seja incluída novamente no roteamento do balanceador de carga.

O Route 53 ARC usa verificações de integridade para afastar o tráfego das zonas de disponibilidade, solicitando que as verificações de integridade sejam definidas como não íntegras e, em seguida, como íntegras novamente quando você cancela uma mudança de zona ou ela expira. No entanto, é importante observar que a mudança de zona não inclui verificações de integridade que monitoram a integridade subjacente dos balanceadores de carga ou aplicativos.

Você deve definir que todas as mudanças de zona expirem quando você as iniciar. Inicialmente, você pode definir uma mudança de zona para expirar em no máximo três dias (72 horas). No entanto, você pode atualizar uma mudança de zona para definir uma nova expiração a qualquer momento. Você também pode cancelar uma mudança de zona antes que ela expire, se estiver pronto para restaurar o tráfego para a zona de disponibilidade.

Em alguns cenários específicos, uma mudança de zona não desloca o tráfego da AZ. Por exemplo, se os grupos de destino do balanceador de carga nas AZs não tiverem nenhuma instância ou se nenhuma das instâncias estiverem íntegras, o balanceador de carga estará em um estado de falha aberta. Se você iniciar uma mudança de zona para um balanceador de carga nesse cenário, ela não alterará quais AZs o balanceador de carga usa porque ele já está em um estado de falha aberta. Esse comportamento é esperado. A mudança de zona não pode forçar uma AZ à não integridade e transferir o tráfego para outras AZs em uma região se todas as AZs falharem na abertura (não integridade). Um segundo cenário é se você iniciar uma mudança de zona para um Application Load Balancer que seja um endpoint para um acelerador no AWS Global Accelerator. A mudança de zona não é compatível com Application Load Balancers, que são endpoints de aceleradores no Global Accelerator.

Para obter mais informações sobre o suporte a mudanças de zona, consulte Recursos compatíveis com mudança de zona e mudança automática de zona.

## Iniciar uma mudança de zona

As etapas desta seção explicam como iniciar uma mudança de zona iniciada pelo cliente no console do Controlador de Recuperação de Aplicações do Amazon Route 53. Para trabalhar com a mudança de zona de forma programática, consulte o Guia de referência da API de mudança de zona.

Como iniciar uma mudança de zona

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança de zona.
3. Na página Mudança de zona, escolha Iniciar mudança de zona.
4. Selecione a zona de disponibilidade da qual você deseja afastar o tráfego.
5. Selecione um balanceador de carga na tabela Recursos para o qual afastar o tráfego.
6. Em Definir expiração da mudança de zona, escolha ou insira uma expiração para a mudança de zona. Uma mudança de zona pode ser configurada para ficar ativa inicialmente por um minuto ou por até três dias (72 horas).

   Todas as mudanças de zona são temporárias. Você deve definir uma expiração, mas pode atualizar as mudanças ativas posteriormente para definir um novo período de expiração de até três dias.
7. Insira um comentário. Você pode atualizar a mudança de zona posteriormente para editar o comentário, se quiser.
8. Marque a caixa de seleção para reconhecer que iniciar uma mudança de zona reduzirá a capacidade disponível para seu aplicativo ao afastar o tráfego da zona de disponibilidade.
9. Escolha Iniciar.

## Atualizar ou cancelar uma mudança de zona

As etapas desta seção explicam como atualizar uma mudança de zona que você inicia ou cancelar uma mudança de zona no console do Controlador de Recuperação de Aplicações do Amazon Route 53. Para trabalhar com a mudança de zona de forma programática, consulte o Guia de referência da API de mudança de zona.

Você pode atualizar uma mudança de zona para definir uma nova expiração, editar ou substituir o comentário pela mudança de zona. Você pode cancelar uma mudança de zona a qualquer momento antes que ela expire.

Você pode cancelar as mudanças de zona que você inicia ou as mudanças de zona que a AWS inicia em um recurso para execução prática em mudança automática de zona.

Como atualizar uma mudança de zona

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança de zona.
3. Selecione uma mudança de zona que você deseja atualizar e escolha Atualizar mudança de zona.
4. Em Definir expiração da mudança de zona, opcionalmente, selecione ou insira uma expiração.
5. Em Comentário, opcionalmente, edite o comentário existente ou insira um novo.
6. Escolha Atualizar.

Como cancelar uma mudança de zona

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança de zona.
3. Selecione uma mudança de zona que você deseja cancelar e, em seguida, escolha Cancelar mudança de zona.
4. Na caixa de diálogo modal de confirmação, escolha Confirmar.

# Recursos compatíveis com mudança de zona e mudança automática de zona

Atualmente, o Controlador de recuperação de aplicações do Amazon Route 53 oferece suporte a mudanças de zona para Network Load Balancers and Application Load Balancers. Há suporte para Network Load Balancers and Application Load Balancers públicos e internos (privados). Você pode iniciar uma mudança de zona para um balanceador de carga no console do Elastic Load Balancing ou no Route 53 ARC.

Analise as seguintes condições para trabalhar com mudanças e recursos de zona no Route 53 ARC:

- A mudança de zona não é compatível com balanceamento de carga entre zonas. Para que um balanceador de carga seja registrado no Route 53 ARC, verifique se você desativou o balanceamento de carga entre zonas para o balanceador de carga no ELB.
- Um recurso deve estar ativo e totalmente provisionado para transferir o tráfego para ele. Antes de iniciar uma mudança de zona para um recurso, verifique se ele é gerenciado no Route 53 ARC. Consulte a lista de recursos gerenciados no AWS Management Console, ou use a operação `get-managed-resource` com o identificador do recurso.
- A mudança de zona não é compatível com os Application Load Balancers, que são endpoints de aceleradores no AWS Global Accelerator.
- Quando um Application Load Balancer for o destino de um Network Load Balancer, inicie a mudança de zona a partir do Network Load Balancer. Se você iniciar a mudança de zona a partir do Application Load Balancer, o Network Load Balancer não interrompe o envio de tráfego para o Application Load Balancer e seus destinos.
- O recurso para uma mudança de zona deve ser um recurso gerenciado que tenha sido registrado no Route 53 ARC por um serviço da AWS. O Elastic Load Balancing se registra automaticamente nos Route 53 ARC Network Load Balancers e Application Load Balancers com o balanceamento de carga entre zonas desativado.
- Para iniciar uma mudança de zona com um recurso, ele deve estar implantado na zona de disponibilidade e na região da AWS em que você iniciar a mudança. Certifique-se de iniciar uma mudança de zona na mesma região em que a AZ da mudança está, e que o recurso para o qual você está transferindo o tráfego também esteja na mesma AZ e região.
- Verifique se o você tem as permissões do IAM corretas para usar a mudança de zona com um recurso. Para ter mais informações, consulte IAM e permissões para mudança de zona.

# Mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53

A mudança automática de zona é um recurso do Controlador de Recuperação de Aplicações do Amazon Route 53. Com a mudança automática de zona, você autoriza a AWS a transferir o tráfego de recursos de uma aplicação de uma zona de disponibilidade durante eventos, em seu nome, para ajudar a reduzir o tempo de recuperação. A AWS inicia uma mudança automática quando a telemetria interna indica que há uma deficiência na zona de disponibilidade que pode afetar potencialmente os clientes. Quando a AWS inicia uma mudança automática, o tráfego da aplicação para os recursos que você configurou para a mudança automática de zona começa a ser transferido para fora da zona de disponibilidade.

Esteja ciente de que o Route 53 ARC não inspeciona a integridade dos recursos individuais. A AWS só inicia uma mudança automática quando a telemetria da AWS detecta que há uma deficiência na zona de disponibilidade capaz de impactar os clientes. Em alguns casos, podem ser transferidos recursos que não estão sofrendo impacto.

Com a mudança automática de zona, você também autoriza a AWS a transferir o tráfego de recursos de uma aplicação de uma zona de disponibilidade, em seu nome, para execuções práticas regulares. As execuções práticas são necessárias para a mudança automática de zona. As mudanças de zona que o Route 53 ARC inicia para execuções práticas ajudam você a garantir que a mudança do tráfego de uma zona de disponibilidade durante uma mudança automática seja segura para a aplicação. As execuções práticas testam regularmente se a aplicação pode operar normalmente sem uma zona de disponibilidade, iniciando mudanças de zona que transferem o tráfego de um recurso para fora de uma zona de disponibilidade. As execuções práticas ocorrem semanalmente e fornecem um resultado, como `SUCCEEDED` ou `FAILED`, para ajudar você a entender se a aplicação funciona conforme o esperado.

> **Important**
>
> Antes de configurar as execuções práticas ou habilitar a mudança automática de zona, é altamente recomendável que você ajuste previamente a escala de capacidade dos recursos da aplicação em todas as zonas de disponibilidade da região em que os recursos da aplicação estão implantados. Você não deve depender da escalabilidade sob demanda quando uma mudança automática ou um treino começa. A mudança automática de zona, incluindo as execuções práticas, funciona de forma independente e não espera a conclusão

das ações de ajuste de escala automático. Depender do ajuste de escala automático, em vez do ajuste prévio, pode resultar em perda de disponibilidade.
Se você usa o ajuste de escala automático para lidar com ciclos regulares de tráfego, é altamente recomendável configurar a capacidade mínima do ajuste de escala automático para continuar operando normalmente com a perda de uma zona de disponibilidade.

Se você planeja habilitar a mudança automática de zona ou configurar execuções práticas, depois de ajustar previamente a escala de capacidade dos recursos da aplicação, teste se a aplicação consegue operar normalmente sem uma zona de disponibilidade. Para testar isso, inicie uma mudança de zona para mover o tráfego de um recurso para fora de uma zona de disponibilidade. Depois de verificar que a aplicação tem capacidade suficiente para continuar operando normalmente, as execuções práticas regulares que o Route 53 ARC realiza ajudam você a confirmar, continuamente, que tem capacidade suficiente para uma mudança automática.

As mudanças automáticas e as mudanças de zona para execução prática são temporárias. Com as mudanças automáticas, quando a zona de disponibilidade afetada se recupera, a AWS para de transferir o tráfego dos recursos para fora da zona de disponibilidade. O tráfego da aplicação para os clientes retorna para todas as zonas de disponibilidade na região. Com uma execução prática, o tráfego de um único recurso é removido de uma zona de disponibilidade por cerca de 30 minutos, depois é transferido de volta para todas as zonas de disponibilidade na região.

Você pode configurar EventBridge as notificações da Amazon para alertá-lo sobre turnos automáticos e treinos. Para ter mais informações, consulte Usando o Route 53 ARC com a Amazon EventBridge.

Tópicos

# Como a mudança automática de zona e as execuções práticas funcionam

O recurso de mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53 permite que a AWS mova o tráfego de um recurso para fora de uma zona de disponibilidade, em seu nome, quando a AWS determinar que há uma deficiência que pode afetar os clientes na zona de disponibilidade. A mudança automática de zona foi projetada para um recurso que tem ajuste de escala prévio em todas as zonas de disponibilidade em uma Região da AWS, para que uma aplicação possa operar normalmente com a perda de uma zona de disponibilidade.

Com a mudança automática de zona, é necessário configurar execuções práticas, nas quais o Route 53 ARC move regularmente o tráfego do recurso para fora de uma zona de disponibilidade. Em geral, o Route 53 ARC agenda execuções práticas semanais para todos os recursos que têm uma configuração de execução prática associada. As execuções práticas são programadas de forma independente para cada recurso.

Para cada execução prática, o Route 53 ARC registra um resultado. Se uma execução prática for interrompida por uma condição de bloqueio, o resultado da execução não será marcado como bem-sucedido. Para obter mais informações sobre os resultados das execuções práticas, consulte Resultados das execuções práticas.

Você pode configurar EventBridge as notificações da Amazon para enviar informações sobre turnos automáticos e treinos. Para ter mais informações, consulte Usando o Route 53 ARC com a Amazon EventBridge.

Tópicos

### Quando a AWS inicia e interrompe as mudanças automáticas

Ao habilitar a mudança automática de zona para um recurso, você autoriza a AWS a mover o tráfego de recursos de uma aplicação para fora de uma zona de disponibilidade durante eventos, em seu nome, com a finalidade de ajudar a reduzir o tempo para recuperação.

Para conseguir isso, a mudança automática de zona usa a telemetria da AWS para detectar, o quanto antes, que há uma deficiência na zona de disponibilidade capaz de impactar os clientes. Quando a AWS inicia uma mudança automática, o tráfego para os recursos configurados começa imediatamente a se deslocar da zona de disponibilidade prejudicada, capaz de impactar os clientes.

A mudança automática de zona é um recurso projetado para clientes que ajustaram previamente a escala dos recursos da aplicação para todas as zonas de disponibilidade em uma Região da AWS. Você não deve depender da escalabilidade sob demanda quando uma mudança automática ou um treino começa.

A AWS encerra uma mudança automática quando determina que a zona de disponibilidade foi recuperada.

### Quando o Route 53 ARC agenda, inicia e encerra as execuções práticas

O Route 53 ARC agenda uma execução prática para um recurso semanalmente, por cerca de 30 minutos. O Route 53 ARC agenda, inicia e gerencia as execuções práticas para cada recurso de forma independente. O Route 53 ARC não agrupa execuções práticas para recursos na mesma conta.

Quando uma execução prática acontece pela duração esperada, sem interrupção, ela é marcada com um resultado `SUCCESSFUL`. Existem vários outros resultados possíveis: `FAILED`, `INTERRUPTED` e `PENDING`. Os valores e as descrições dos resultados estão incluídos na seção Resultados das execuções práticas.

Há alguns cenários em que o Route 53 ARC interrompe uma execução prática e a encerra. Por exemplo, se uma mudança automática começar durante uma execução prática, o Route 53 ARC interromperá a execução prática e a encerrará. Como outro exemplo, digamos que o recurso tenha uma resposta adversa a uma execução prática e faça com que um alarme que você especificou para monitorar a execução prática entre em um estado `ALARM`. Nesse cenário, o Route 53 ARC também interromperá a execução prática e a encerrará.

Além disso, há vários cenários em que o Route 53 ARC não inicia uma execução prática programada para um recurso.

Em resposta às execuções práticas interrompidas e bloqueadas de um recurso, o Route 53 ARC faz o seguinte:

- Se uma execução prática de um recurso for interrompida enquanto estiver em andamento, o Route 53 ARC considerará que a execução prática semanal terminou e agendará uma nova execução prática para o recurso na semana seguinte. O resultado da prática semanal será `INTERRUPTED` nesse cenário, não `FAILED`. O resultado da execução prática é definido como `FAILED` somente quando o alarme de resultado que monitora a execução prática entra em um estado `ALARM` durante a execução prática.
- Se houver uma restrição de bloqueio quando uma execução prática de um recurso estiver programada para ser iniciada, o Route 53 ARC não iniciará a execução prática. O Route 53 ARC continua realizando o monitoramento regularmente a fim de determinar se ainda há uma ou mais restrições de bloqueio. Quando não houver nenhuma restrição de bloqueio, o Route 53 ARC iniciará a execução prática do recurso.

Veja a seguir exemplos de restrições de bloqueio que impedem que o Route 53 ARC inicie ou dê continuidade a uma execução prática para um recurso:

- O Route 53 ARC não inicia nem dá continuidade a execuções práticas quando há um experimento do AWS Fault Injection Service em andamento. Se um evento do AWS FIS estiver ativo no início de uma execução prática, o Route 53 ARC não iniciará a execução prática. O Route 53 ARC monitora as restrições de bloqueio durante as execuções práticas, incluindo um evento do AWS FIS. Se um evento do AWS FIS começar enquanto uma execução prática estiver ativa, o Route 53 ARC encerrará a execução prática e não tentará iniciar outra até a próxima execução prática programada regularmente para o recurso.
- Se houver um evento do AWS atual em uma região, o Route 53 ARC não iniciará execuções práticas para recursos e encerrará as execuções práticas ativas na região.

Quando a execução prática termina sem ser interrompida, o Route 53 ARC agenda a próxima execução prática na semana seguinte, como de costume. Se uma execução prática não for iniciada devido a uma restrição de bloqueio, como um experimento do AWS FIS ou uma janela de tempo bloqueada que você especificou, o Route 53 ARC continuará tentando iniciar a execução prática até que ela possa ser iniciada.

Precedência para mudanças de zona, execuções práticas e mudanças automáticas

Não pode haver mais do que uma mudança de tráfego em vigor ao mesmo tempo para um recurso, ou seja, apenas uma mudança de zona para execução prática, uma mudança de zona iniciada pelo cliente ou uma mudança automática para o recurso. Quando houver mais de uma

mudança de tráfego em andamento, o Route 53 ARC seguirá uma precedência para determinar qual mudança de tráfego estará em vigor para um recurso.

O princípio geral de precedência é que as mudanças de zona que você inicia como cliente têm precedência sobre as mudanças automáticas, que têm precedência sobre as execuções práticas. Ou seja, mudanças de zona iniciadas pelo cliente **>** mudanças automáticas **>** mudanças de zona para execução prática.

Para ilustrar isso, veja a seguir como a precedência funciona em alguns cenários de exemplo:

- Se houver uma mudança automática ativa e você iniciar uma mudança de zona para um recurso que tenha a mudança automática habilitada, a mudança de zona iniciada por você será `APPLIED`. O recurso agora é transferido para fora da zona de disponibilidade à qual a mudança de zona se aplica. Se a mudança de zona terminar antes de a AWS encerrar a mudança automática, a mudança automática se tornará a mudança `APPLIED`. Portanto, o recurso é transferido para fora da zona de disponibilidade em que a AWS está com a mudança automática em andamento.
- Se houver uma mudança de zona ativa que você iniciou para um recurso que tem a mudança automática habilitada e a AWS iniciar uma mudança automática, a mudança automática existirá para o recurso. No entanto, a mudança de zona será definida como `APPLIED` e a mudança automática será definida como `NOT APPLIED` até que a mudança de zona termine. Depois, o status da mudança automática será atualizado para `APPLIED` e a mudança automática transferirá o tráfego para o recurso até a AWS encerrar a mudança automática.
- Se houver uma execução prática ativa para um recurso e você iniciar uma mudança de zona para esse recurso que transfira o tráfego para fora da mesma zona de disponibilidade, a execução prática será interrompida. Se você iniciar uma mudança de zona que transfira o tráfego para fora de uma zona de disponibilidade diferente, a execução prática continuará normalmente.
- Se houver uma mudança de zona ativa para um recurso e o Route 53 ARC estiver programado para iniciar uma execução prática, a execução prática será adiada por uma hora. Depois, o Route 53 ARC tentará iniciar a execução prática novamente. O Route 53 ARC continuará verificando de hora em hora até que a execução prática possa ser iniciada.

A mudança de tráfego atualmente em vigor para o recurso tem um status de mudança de zona definido como `APPLIED`. Somente uma mudança é definida como `APPLIED` por vez. Outras mudanças que estão em andamento são definidas como `ACTIVE`.

Interromper uma mudança automática ativa ou uma execução prática de um recurso

Para interromper uma mudança automática em andamento para um recurso, desabilite a mudança automática de zona para o recurso.

Quando você desabilita a mudança automática de zona, a configuração de execução prática do recurso não é afetada. As execuções práticas regulares ainda ocorrem para o recurso, no mesmo cronograma. Se quiser interromper as execuções práticas além de desabilitar as mudanças automáticas, será necessário excluir a configuração de execução prática associada ao recurso.

Quando você exclui uma configuração de execução prática, a AWS interrompe a realização semanal de execuções práticas que transferem o tráfego do recurso para fora de uma zona de disponibilidade. Além disso, como a mudança automática de zona exige execuções práticas, quando você exclui uma configuração de execução prática usando o console do Route 53 ARC, essa ação também desabilita a mudança automática de zona para o recurso. No entanto, observe que, se você usar a API de mudança automática de zona para excluir uma execução prática, primeiro desabilite a mudança automática de zona para o recurso.

Para interromper uma execução prática ativa, cancele a mudança de zona para execução prática. Para ter mais informações, consulte Cancelar uma mudança de zona para execução prática.

Como o tráfego é transferido

Para mudanças automáticas e mudanças de zona para execução prática, o tráfego é transferido para fora de uma zona de disponibilidade usando o mesmo mecanismo que o Route 53 ARC usa para mudanças de zona iniciadas pelo cliente. Para transferir o tráfego para fora de uma zona de disponibilidade para balanceadores de carga que têm o balanceamento de carga entre zonas desativado, o Route 53 ARC define a verificação de integridade do balanceador de carga para a zona de disponibilidade como não íntegra, de modo que sua verificação de integridade falhe. Uma verificação de integridade, por sua vez, faz com que o Amazon Route 53 retire os endereços IP correspondentes do recurso do DNS, de forma que o tráfego seja redirecionado da zona de disponibilidade. Em vez disso, novas conexões agora são roteadas para outras zonas de disponibilidade na Região da AWS.

Com uma mudança automática, quando uma zona de disponibilidade se recupera e a AWS decide encerrar a mudança automática, o Route 53 ARC reverte o processo de verificação de integridade, solicitando que as verificações de integridade do Route 53 sejam revertidas. Depois, os endereços IP de zona originais são restaurados e, se as verificações de integridade continuarem íntegras, a zona de disponibilidade será incluída novamente no roteamento do balanceador de carga.

É importante estar ciente de que as mudanças automáticas não se baseiam em verificações de integridade que monitoram a integridade subjacente dos balanceadores de carga ou das aplicações. O Route 53 ARC usa verificações de integridade para transferir o tráfego para fora das zonas de disponibilidade, solicitando que as verificações de integridade sejam definidas como não íntegras, depois restaura as verificações de integridade como normais novamente quando encerra uma mudança automática ou mudança de zona.

Alarmes para execuções práticas

Você pode especificar dois CloudWatch alarmes para treinos em deslocamento automático zonal. O primeiro alarme, o alarme de resultado, é necessário. Você deve configurar o alarme de resultado para monitorar a integridade da aplicação quando o tráfego é transferido para fora de uma zona de disponibilidade durante cada execução prática de 30 minutos.

Para que uma execução prática seja eficaz, especifique como alarme de resultado um CloudWatch alarme que monitora as métricas do recurso, ou do seu aplicativo, que respondem com um `ALARM` estado em que seu aplicativo é afetado adversamente pela perda de uma zona de disponibilidade. Para obter mais informações, consulte a seção Alarmes que você especifica para execuções práticas em Considerações ao configurar a mudança automática de zona.

O alarme de resultado também fornece informações sobre o resultado da execução prática que o Route 53 ARC reporta para cada execução prática. Se o alarme entrar em um estado `ALARM`, a execução prática será encerrada e seu resultado será retornado como `FAILED`. Se a execução prática concluir o período de teste programado de 30 minutos e o alarme de resultado não entrar em um estado `ALARM`, o resultado será retornado como `SUCCEEDED`. Uma lista de todos os valores de resultados, com descrições, é fornecida na seção Resultados das execuções práticas.

Opcionalmente, você pode especificar um segundo alarme, o alarme de bloqueio. O alarme de bloqueio impede o início ou a continuidade de execuções práticas quando está em um estado `ALARM`. Esse alarme impede o início de mudanças de tráfego para execução prática e interrompe todas as execuções práticas em andamento quando está em um estado `ALARM`.

Por exemplo, em uma arquitetura grande com vários microsserviços, quando um microsserviço está enfrentando um problema, você normalmente deseja interromper todas as outras alterações no ambiente da aplicação, incluindo o bloqueio de execuções práticas.

Datas bloqueadas e janelas bloqueadas (UTC)

Você tem a opção de bloquear as execuções práticas para datas específicas do calendário ou para janelas de tempo específicas, ou seja, dias e horários, em UTC.

Por exemplo, se você tiver uma atualização de aplicação programada para ser lançada em 1.º de maio de 2024 e não quiser que as execuções práticas movam o tráfego naquele momento, poderá definir uma data de bloqueio para `2024-05-01`.

Por outro lado, digamos que você faça resumos de relatórios comerciais três dias por semana. Para esse cenário, você pode definir os seguintes dias e horários recorrentes como janelas bloqueadas, em UTC: `MON-20:30-21:30 WED-20:30-21:30 FRI-20:30-21:30`.

# Considerações ao configurar a mudança automática de zona

A mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53 inclui dois tipos de mudanças de tráfego: mudanças automáticas e mudanças de zona para execução prática. Com uma mudança automática, a AWS ajuda a reduzir o tempo de recuperação, transferindo o tráfego de recursos da aplicação para fora de uma zona de disponibilidade durante eventos, em seu nome. Com as execuções práticas, o Route 53 ARC inicia uma mudança de zona para transferir o tráfego para fora de uma zona de disponibilidade para um recurso e vice-versa, em uma cadência semanal. As execuções práticas ajudam você a garantir que tenha aumentado a escala vertical de capacidade suficiente das zonas de disponibilidade em uma região para que a aplicação tolere a perda de uma zona de disponibilidade.

Há várias considerações a serem lembradas a respeito das mudanças automáticas e execuções práticas. Analise os tópicos a seguir antes de habilitar a mudança automática de zona ou configurar execuções práticas para um recurso.

Tópicos



Ajuste prévio da escala de capacidade dos recursos

Quando a AWS transfere o tráfego para fora de uma zona de disponibilidade, é importante que as demais zonas de disponibilidade possam atender ao aumento das taxas de solicitação do recurso. Esse padrão é conhecido como estabilidade estática. Para obter mais informações,

consulte o whitepaper Estabilidade estática usando zonas de disponibilidade na Amazon Builders' Library.

Por exemplo, se uma aplicação precisar de 30 instâncias para atender os clientes, você deverá provisionar 15 instâncias em três zonas de disponibilidade, totalizando 45 instâncias. Ao fazer isso, quando a AWS transferir o tráfego para fora de uma zona de disponibilidade, seja com uma mudança automática ou durante uma execução prática, a AWS ainda conseguirá atender os clientes da aplicação com o total restante de 30 instâncias em duas zonas de disponibilidade.

O recurso de mudança automática de zona no Route 53 ARC ajuda você a se recuperar rapidamente de eventos da AWS em uma zona de disponibilidade quando você tem uma aplicação com recursos previamente ajustados para funcionar normalmente com a perda de uma zona de disponibilidade. Antes de habilitar a mudança automática de zona para um recurso, ajuste a escala de capacidade do recurso em todas as zonas de disponibilidade configuradas em uma Região da AWS. Depois, inicie as mudanças de zona para o recurso a fim de testar se a aplicação ainda funciona normalmente quando o tráfego é transferido para fora de uma zona de disponibilidade.

Depois de realizar testes com mudanças de zona, habilite a mudança automática de zona e configure execuções práticas para os recursos da aplicação. As execuções práticas regulares com mudança automática de zona ajudam você a garantir, continuamente, que a capacidade ainda seja dimensionada adequadamente. Com capacidade suficiente em todas as zonas de disponibilidade, a aplicação pode continuar atendendo os clientes, sem interrupção, durante uma mudança automática.

Para obter mais informações sobre como iniciar uma mudança de zona para um recurso, consulte Mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53.

### Tipos de recursos e restrições

A mudança automática de zona oferece suporte à transferência do tráfego para fora de uma zona de disponibilidade para todos os recursos que são compatíveis com a mudança de zona. Em geral, há suporte para Network Load Balancers e Application Load Balancers com balanceamento de carga entre zonas desativado. Em alguns cenários de recursos específicos, a mudança automática de zona não transfere o tráfego para fora de uma zona de disponibilidade para uma mudança automática.

Por exemplo, se os grupos de destino do balanceador de carga nas zonas de disponibilidade não tiverem nenhuma instância ou se nenhuma das instâncias estiverem íntegras, o balanceador

de carga estará em um estado de falha aberta. Se a AWS iniciar uma mudança automática para um balanceador de carga nesse cenário, a mudança automática não alterará quais zonas de disponibilidade o balanceador de carga usa porque ele já está em um estado de falha aberta. Esse comportamento é esperado. A mudança automática não pode causar problemas de integridade em uma zona de disponibilidade e transferir o tráfego para outras zonas de disponibilidade em uma Região da AWS em caso de falha na abertura de todas as zonas de disponibilidade (não íntegras).

Um segundo cenário é se a AWS iniciar uma mudança automática para um Application Load Balancer que é um endpoint para um acelerador no AWS Global Accelerator. Assim como no caso da mudança de zona, a mudança automática não é compatível com Application Load Balancers que são endpoints de aceleradores no Global Accelerator.

Para conferir detalhes sobre os recursos compatíveis, incluindo todos os requisitos e exceções que você deve conhecer, consulte Recursos compatíveis com mudança de zona e mudança automática de zona.

Alarmes que você especifica para execuções práticas

Ao considerar como configurar CloudWatch alarmes para ensaios práticos para seu recurso, lembre-se do seguinte:

- Para o alarme de resultado, que é obrigatório, recomendamos que você configure um CloudWatch alarme para entrar em um `ALARM` estado em que as métricas do recurso ou do seu aplicativo indiquem que o deslocamento do tráfego para fora da Zona de Disponibilidade afeta negativamente o desempenho. Por exemplo, você pode determinar um limite para as taxas de solicitação do recurso, depois configurar um alarme para entrar em um estado `ALARM` quando o limite for excedido. Você é responsável por configurar um alarme apropriado que faça com que a AWS encerre a execução prática e retorne um resultado `FAILED`.
- Recomendamos que você siga o AWSWell Architected Framework, que recomenda a implementação de indicadores-chave de desempenho (KPIs) como alarmes. CloudWatch Se você fizer isso, poderá usar esses alarmes para criar um alarme composto para ser usado como gatilho de segurança, a fim de evitar que as execuções práticas sejam iniciadas caso elas possam fazer com que a aplicação perca um KPI. Quando o alarme sair de um estado `ALARM`, o Route 53 ARC iniciará as execuções práticas na próxima vez que uma execução prática estiver agendada para o recurso.
- Para o alarme de bloqueio de execução prática, caso opte por configurá-lo, você poderá escolher rastrear uma métrica específica usada para indicar que não deseja que uma execução prática seja iniciada.

- Para alarmes de execução prática, você especifica o Amazon Resource Name (ARN) para cada alarme, que deve ser configurado primeiro na Amazon. CloudWatch Os CloudWatch alarmes que você especifica podem ser alarmes compostos, para permitir que você inclua várias métricas e verificações para seu aplicativo e recurso que podem fazer com que o alarme entre em um estado. `ALARM` Para obter mais informações, consulte Combinação de alarmes no Guia do CloudWatch usuário da Amazon.
- Certifique-se de que os CloudWatch alarmes que você especifica para os treinos estejam na mesma região do recurso para o qual você está configurando um treino.

Resultados das execuções práticas

Para cada execução prática, o Route 53 ARC relata um resultado. Veja a seguir os possíveis resultados para uma execução prática:

- BEM-SUCEDIDA: o alarme de resultado não entrou em um estado `ALARM` durante a execução prática e ela concluiu todo o período de teste de 30 minutos.
- FALHOU: o alarme de resultado entrou em um estado `ALARM` durante a execução prática.
- INTERROMPIDA: a execução prática foi encerrada por um motivo que não foi o alarme de resultado entrando em um estado `ALARM`. Uma execução prática pode ser interrompida por vários motivos, inclusive pelos seguintes:
  - A execução prática foi encerrada porque a AWS iniciou uma mudança automática na Região da AWS ou houve uma condição de alarme na região.
  - A execução prática foi encerrada porque a configuração da execução prática foi excluída do recurso.
  - A execução prática foi encerrada porque o cliente iniciou uma mudança de zona para o recurso na zona de disponibilidade da qual a mudança de zona para execução prática estava transferindo o tráfego.
  - A execução prática foi encerrada porque um CloudWatch alarme especificado para a configuração da execução prática não pode mais ser acessado.
  - A execução prática foi encerrada porque o alarme de bloqueio especificado para a execução prática entrou em um estado `ALARM`.
  - A execução prática foi encerrada por um motivo desconhecido.
- PENDENTE: a execução prática está ativa (em andamento). Ainda não há resultado a ser retornado.

# Habilitar ou desabilitar a mudança automática de zona

As etapas desta seção explicam como habilitar ou desabilitar a mudança automática de zona no console do Controlador de Recuperação de Aplicações do Amazon Route 53. Para trabalhar com a mudança automática de zona de forma programática, consulte o Guia de referência da API de mudança de zona e mudança automática de zona.

Quando a mudança automática de zona é habilitada, você autoriza a AWS a transferir o tráfego de recursos da aplicação para fora de uma zona de disponibilidade durante eventos, em seu nome, para ajudar a reduzir o tempo de recuperação.

Como habilitar ou desabilitar a mudança automática de zona

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança automática de zona.
3. Em Configurações da mudança automática de zona de recursos, escolha um recurso.
4. No menu Ações, escolha Habilitar mudança automática de zona ou Desabilitar mudança automática de zona e siga as etapas para concluir a atualização.

Se o recurso não tiver uma configuração de execução prática, a opção Habilitar mudança automática de zona não estará disponível. Para configurar uma configuração de execução prática e habilitar a mudança automática de zona, escolha Configurar mudança automática de zona.

# Configurar, editar ou excluir uma configuração de execução prática

As etapas desta seção explicam como editar ou excluir uma configuração de execução prática no console do Controlador de Recuperação de Aplicações do Amazon Route 53. Para trabalhar com a mudança automática de zona de forma programática, incluindo alterações nas configurações de execução prática, consulte o Guia de referência da API de mudança de zona e mudança automática de zona.

Se você excluir uma configuração de execução prática no console, a mudança automática de zona será desabilitada. Antes de excluir uma configuração de execução prática com uma operação de API, é necessário desabilitar a mudança automática de zona. Você pode configurar uma execução prática sem habilitar a mudança automática de zona. No entanto, para que a mudança automática

de zona seja habilitada para um recurso, é necessário ter uma execução prática configurada para o recurso.

Como configurar uma execução prática

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança automática de zona.
3. Escolha Configurar mudança automática de zona.
4. Escolha um recurso a ser configurado para a mudança automática de zona.
5. Desabilite a mudança automática de zona se não quiser que a AWS inicie uma mudança automática para um recurso quando houver um evento da AWS. Você pode continuar com o assistente para definir uma configuração de execução prática sem habilitar mudanças automáticas, se quiser.
6. Escolha opções de execução prática para o recurso. Para alarmes, você pode fazer o seguinte:

   - (Obrigatório) Especifique um alarme de resultado para monitorar as execuções práticas desse recurso.
   - (Opcional) Especifique um alarme de bloqueio para as execuções práticas desse recurso.

   Para obter mais informações, consulte a seção Alarmes que você especifica para execuções práticas em Considerações ao configurar a mudança automática de zona.
7. Opcionalmente, especifique datas e janelas bloqueadas. Escolha datas ou janelas (dias e horas) para impedir que o Route 53 ARC inicie execuções práticas para esse recurso. Todas as datas e horas são mostradas em UTC.
8. Marque a caixa de seleção para confirmar que você leu a mensagem de confirmação.
9. Selecione Create.

Como editar uma configuração de execução prática

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança automática de zona.
3. Em Configurações da mudança automática de zona de recursos, escolha um recurso.
4. No menu Ações, escolha Editar configuração da execução prática.

5. Faça alterações na configuração da execução prática para realizar uma ou mais das seguintes ações:

   - Para alarmes, você pode fazer o seguinte:
     - Para o alarme de bloqueio, você pode adicionar um alarme, excluir o alarme ou especificar um alarme de bloqueio diferente.
     - Para o alarme de resultado que monitora os treinos, você pode especificar um CloudWatch alarme diferente para usar. Os alarmes de resultado são obrigatórios, portanto, você não pode excluí-los.
   - Para datas bloqueadas e janelas bloqueadas, você pode adicionar novas datas ou dias e horas, ou pode remover ou atualizar datas ou dias e horas existentes. Todas as datas e horas são mostradas em UTC.
6. Escolha Salvar.

Como excluir uma configuração de execução prática

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança automática de zona.
3. Em Configurações da mudança automática de zona de recursos, escolha um recurso.
4. No menu Ações, escolha Excluir configuração da execução prática.
5. Na caixa de diálogo modal de confirmação, digite `Delete` e selecione Excluir.

   Observe que a exclusão de uma configuração de execução prática no console também desabilita a mudança automática de zona para o recurso. A mudança automática de zona exige que uma execução prática seja configurada para o recurso.

# Cancelar uma mudança de zona para execução prática

As etapas desta seção explicam como cancelar uma mudança de zona no console do Controlador de Recuperação de Aplicações do Amazon Route 53. Para trabalhar com a mudança de zona e a mudança automática de zona de forma programática, consulte o Guia de referência da API de mudança de zona e mudança automática de zona.

Você pode cancelar as mudanças de zona que você inicia ou as mudanças de zona que a AWS inicia em um recurso para execução prática em mudança automática de zona.

Como cancelar uma mudança de zona para execução prática

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança de zona.
3. Selecione uma mudança de zona que você deseja cancelar e, em seguida, escolha Cancelar mudança de zona.
4. Na caixa de diálogo modal de confirmação, escolha Confirmar.

# Verificação de prontidão do Controlador de recuperação de aplicações do Amazon Route 53

Este capítulo explica como modelar seu aplicativo no Controlador de recuperação de aplicações do Amazon Route 53 criando um grupo de recuperação e células e, em seguida, como adicionar escopos e verificações de prontidão para que o Route 53 ARC audite seu aplicativo.

Depois de criar verificações de prontidão, é possível monitorar o status de prontidão dos recursos. As verificações de prontidão ajudam a garantir que a réplica do aplicativo em espera e seus recursos correspondam continuamente à réplica de produção, refletindo a capacidade, as políticas de roteamento e outros detalhes de configuração do seu aplicativo de produção. Caso contrário, você pode adicionar capacidade ou alterar uma configuração para que as réplicas sejam alinhadas novamente.

> **Important**
>
> As verificações de prontidão são úteis para verificar continuamente se as configurações da réplica do aplicativo e os estados de runtime estão alinhados. As verificações de prontidão não devem ser usadas para indicar se a réplica de produção está íntegra, nem você deve confiar nas verificações de prontidão como principal gatilho para o failover durante um evento de desastre.

Uma verificação de prontidão no Route 53 ARC audita continuamente (em intervalos de um minuto) as incompatibilidades na capacidade da AWS provisionada, cotas de serviço, controles de utilização, discrepâncias de configuração e versão dos recursos incluídos na verificação. As verificações de prontidão podem notificá-lo sobre essas diferenças para garantir que cada réplica tenha a mesma configuração e o mesmo estado de runtime. Embora as verificações de prontidão garantam que suas capacidades configuradas em todas as réplicas sejam consistentes, você não deve esperar que elas decidam qual será a capacidade da réplica. Por exemplo, você deve entender os requisitos do seu aplicativo para dimensionar seus grupos de Auto Scaling com capacidade de buffer suficiente em cada réplica para gerenciar se outra célula não estiver disponível.

Para cotas, quando o Route 53 ARC detecta uma incompatibilidade com uma verificação de prontidão, ele pode tomar medidas para alinhar as cotas das réplicas aumentando a cota mais baixa para corresponder à cota mais alta. Quando as cotas coincidem, o status da verificação de prontidão

é exibido como READY. (Observe que esse não é um processo de atualização imediato e o tempo total depende do tipo de recurso específico e de outros fatores.)

A primeira etapa é configurar verificações de prontidão Como criar um grupo de recuperação que represente seu aplicativo. Cada grupo de recuperação inclui células para cada unidade individual de contenção de falhas ou uma réplica do seu aplicativo. Em seguida, você cria conjuntos de recursos para cada tipo de recurso em seu aplicativo e associa as verificações de prontidão aos conjuntos de recursos. Por fim, você associa os recursos aos escopos de prontidão, para obter o status de prontidão sobre os recursos em um grupo de recuperação (seu aplicativo) ou em células individuais (réplicas, que são regiões ou zonas de disponibilidade).

A prontidão (ou seja, READY ou NOT READY) é baseada nos recursos que estão no escopo da verificação de prontidão e no conjunto de regras para um tipo de recurso. Há conjuntos de regras de prontidão para cada tipo de recurso, que as verificações do Route 53 ARC usam para auditar a disponibilidade dos recursos. O fato de um recurso ser exibido como READY ou não é baseado em como cada regra de prontidão está definida. Todas as regras de prontidão avaliam os recursos, mas algumas comparam os recursos entre si e outras analisam informações específicas sobre cada recurso no conjunto de recursos.

Ao adicionar verificações de prontidão, você pode monitorar o status de prontidão de várias maneiras: com EventBridge, no ou usando as AWS Management Console ações da API ARC do Route 53. Você também pode monitorar o status de prontidão dos recursos em diferentes contextos, incluindo a prontidão das células e do aplicativo. Use o recurso de autorização entre contas no Route 53 ARC para facilitar a configuração e o monitoramento de recursos distribuídos a partir de uma única conta da AWS.

Tópicos

- Verificações de prontidão e cenários de recuperação de desastres
- Verificações de prontidão, conjuntos de recursos e escopos de prontidão
- Como as regras de prontidão determinam o estado
- Verificações de prontidão de recursos de destino do DNS: auditando a prontidão de resiliência
- Criar, atualizar e excluir grupos de recuperação no Route 53 ARC
- Criar e atualizar verificações de prontidão no Route 53 ARC
- Monitorar o status de prontidão no Route 53 ARC
- Descrições das regras de prontidão no Route 53 ARC
- Tipos de recursos e formatos ARN no Route 53 ARC

- Obter recomendações de arquitetura no Route 53 ARC
- Criar autorizações entre contas no Route 53 ARC

# Verificações de prontidão e cenários de recuperação de desastres

As verificações de prontidão do Route 53 ARC fornecem insights sobre se as aplicações e os recursos estão prontos para recuperação, ajudando a garantir que as aplicações sejam escaladas para lidar com o tráfego de failover. Os status de verificação de prontidão não devem ser usados como um sinal para indicar que uma réplica de produção está íntegra. No entanto, você pode usar as verificações de prontidão como um complemento aos sistemas de monitoramento de aplicativos e infraestrutura ou de verificação de integridade para determinar se uma réplica falhará ou se ocorrerá uma falha.

Em uma situação urgente ou em uma interrupção, use uma combinação de verificações de integridade e outras informações para determinar se sua espera está escalada, íntegra e pronta para o failover do tráfego de produção. Por exemplo, verifique se os canários que funcionam na célula em espera estão atendendo aos critérios de sucesso, além de verificar se os estados da verificação de prontidão para a célula em espera estão `READY`.

Note que as verificações de prontidão do Route 53 ARC são hospedadas em uma única região da AWS, Oeste dos EUA (Oregon), e durante uma interrupção ou desastre, as informações de verificação de prontidão podem ficar obsoletas ou as verificações podem ficar indisponíveis. Para ter mais informações, consulte Planos de controle e planos de dados para o Route 53 ARC.

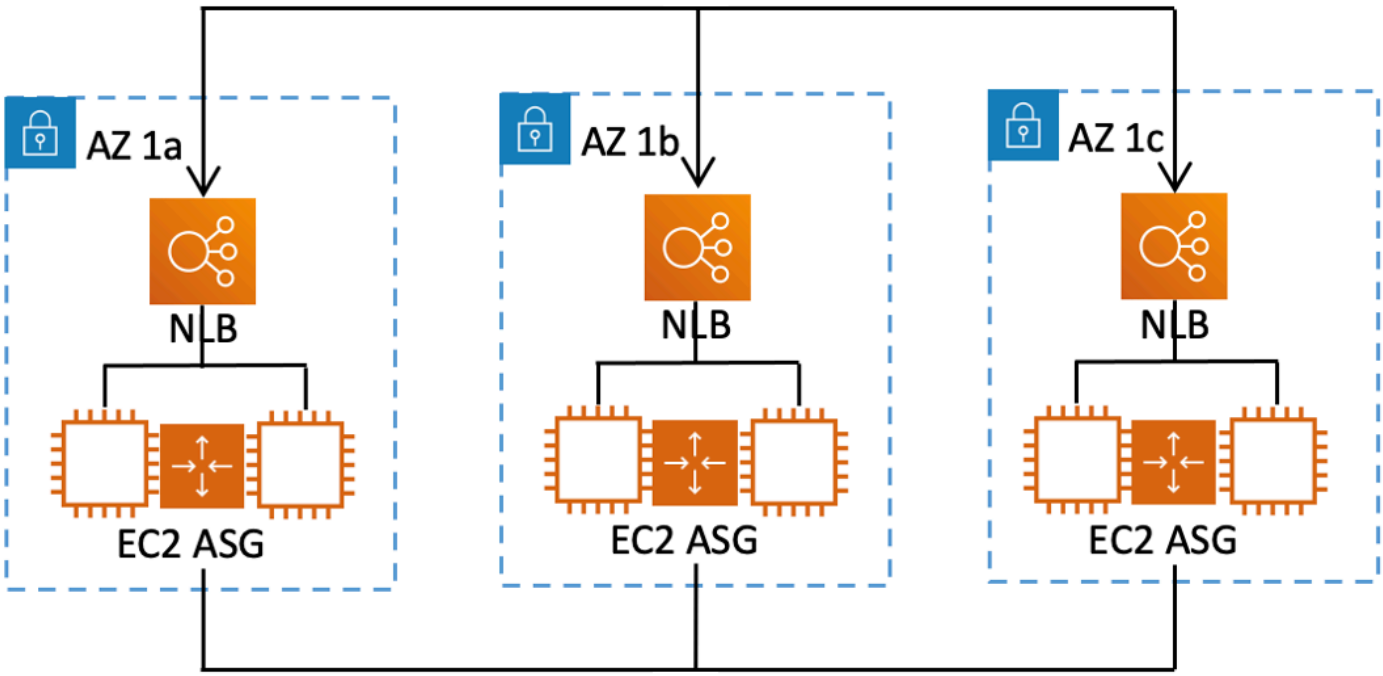
# Verificações de prontidão, conjuntos de recursos e escopos de prontidão

As verificações de prontidão sempre auditam grupos de recursos em conjuntos de recursos. Você cria conjuntos de recursos (separadamente ou enquanto cria uma verificação de prontidão) para agrupar os recursos nas células (zonas de disponibilidade ou regiões da AWS) em seu grupo de recuperação do Route 53 ARC, para então definir verificações de prontidão. Um conjunto de recursos geralmente é um grupo do mesmo tipo de recursos (como Network Load Balancers), mas também pode ser um recurso de destino do DNS, para verificações de prontidão arquitetônica.

Normalmente, você cria um conjunto de recursos e verifica a prontidão para cada tipo de recurso em seu aplicativo. Para verificar a prontidão da arquitetura, você cria um recurso de destino de DNS

de nível superior e um conjunto de recursos global (nível de grupo de recuperação) para ele e, em seguida, cria recursos de destino de DNS em nível de célula para um conjunto de recursos separado.

O diagrama a seguir mostra um exemplo de um grupo de recuperação com três células (zonas de disponibilidade), cada uma com um Network Load Balancer (NLB) e um grupo do Auto Scaling (ASG).




Nesse cenário, você criaria um conjunto de recursos e uma verificação de prontidão para os três Network Load Balancers e um conjunto de recursos e uma verificação de prontidão para os três grupos do Auto Scaling. Agora você tem uma verificação de prontidão para cada conjunto de recursos do seu grupo de recuperação, por tipo de recurso.

Ao criar escopos de prontidão para recursos, você pode adicionar resumos de verificação de prontidão para células ou grupos de recuperação. Para especificar um escopo de prontidão para um recurso, você associa o ARN da célula ou do grupo de recuperação a cada recurso em um conjunto de recursos. Você pode fazer isso ao criar uma verificação de prontidão para um conjunto de recursos.

Por exemplo, ao adicionar uma verificação de prontidão para um conjunto de recursos para os Network Load Balancers desse grupo de recuperação, você pode adicionar escopos de prontidão para cada NLB ao mesmo tempo. Neste caso, você associaria o ARN da AZ 1a ao NLB na AZ 1a, o ARN da `AZ 1b` ao NLB da `AZ 1b`, e o ARN da `AZ 1c` ao NLB da `AZ 1c`. Ao criar uma verificação de

prontidão para os grupos do Auto Scaling, você faria o mesmo, atribuindo escopos a cada um deles ao criar a verificação de prontidão para o conjunto de recursos.

É opcional associar escopos ao criar uma verificação de prontidão. No entanto, é altamente recomendável defini-los. Os escopos de prontidão permitem que o Route 53 ARC mostre os estados corretos `READY` ou `NOT READY` para resumos de grupos de recuperação e verificações de prontidão no nível da célula. A menos que você defina escopos de prontidão, o Route 53 ARC não pode fornecer esses resumos.

Observe que, ao adicionar um recurso global ou no nível do aplicativo, como uma política de roteamento de DNS, você não escolhe um grupo ou célula de recuperação para o escopo de prontidão. Em vez disso, você escolhe o recurso global (sem célula).

## Como as regras de prontidão determinam o estado

As verificações de prontidão do Route 53 ARC determinam o status de prontidão com base nas regras predefinidas para cada tipo de recurso e na forma como essas regras são definidas. O Route 53 ARC inclui um grupo de regras para cada tipo de recurso que ele suporta. Por exemplo, o Route 53 ARC tem grupos de regras de prontidão para clusters do Amazon Aurora, grupos do Auto Scaling e assim por diante. Algumas regras de prontidão comparam recursos em um conjunto, e algumas analisam informações específicas no conjunto de recursos.

Você não pode adicionar, editar ou remover regras de prontidão ou grupos de regras. No entanto, você pode criar um CloudWatch alarme da Amazon e criar uma verificação de prontidão para monitorar o estado do alarme. Por exemplo, você pode criar um CloudWatch alarme personalizado para monitorar os serviços de contêineres do Amazon EKS e criar uma verificação de prontidão para auditar o status de prontidão do alarme.

Você pode visualizar todas as regras de prontidão para cada tipo de recurso do AWS Management Console ao criar um conjunto de recursos, ou pode ver as regras de prontidão posteriormente navegando até a página de detalhes de um conjunto de recursos. Você também pode ver as regras de prontidão na seção a seguir: Regras de prontidão no Route 53 ARC.

Quando uma verificação de prontidão audita um conjunto de recursos com um conjunto de regras, a forma como cada regra é definida determina se o resultado será `READY` ou `NOT READY` para todos os recursos ou se o resultado será diferente para recursos distintos. Além disso, você pode visualizar o status de prontidão de várias maneiras. Por exemplo, você pode ver o status de prontidão de um grupo de recursos em um conjunto ou ver um resumo do status para um grupo de recuperação, uma

célula (uma região da AWS ou zona de disponibilidade, dependendo de como você configurou seu grupo de recuperação).

O texto na descrição de cada regra explica como ela avalia os recursos para determinar o status de prontidão quando essa regra é aplicada. Uma regra é definida para inspecionar cada recurso ou para inspecionar todos os recursos em um conjunto de recursos e determinar a prontidão. Especificamente, as regras funcionam da seguinte forma:

- A regra inspeciona cada recurso no conjunto para garantir uma condição.
  - Se todos os recursos forem bem-sucedidos, todos serão definidos como `READY`.
  - Se um recurso falhar, será definido como `NOT READY` e as outras células permanecerão `READY`.

  Por exemplo: MskClusterState: inspeciona cada cluster do Amazon MSK para garantir que ele esteja em um estado `ACTIVE`.
- A regra inspeciona todos os recursos no conjunto para garantir uma condição.
  - Se a condição for garantida, todos os recursos serão definidos como `READY`.
  - Se algum deles não atender à condição, todos os recursos serão definidos como `NOT READY`.

  Por exemplo: VpcSubnetCount: inspeciona todas as VPC sub-redes para garantir que tenham o mesmo número.
- Regra não crítica: a regra inspeciona todos os recursos no conjunto para garantir uma condição.
  - Se houver falha, o status de prontidão permanece inalterado. Uma regra com esse comportamento tem uma nota em sua descrição.

  Por exemplo: ElbV2CheckAzCount: inspeciona cada Network Load Balancer para garantir que esteja conectado a apenas uma zona de disponibilidade. Nota: essa regra não afeta o status de prontidão.

Além disso, o Route 53 ARC dá um passo extra para cotas. Se uma verificação de prontidão detectar uma incompatibilidade entre células para cotas de serviço (o valor máximo para criação e operações de recursos) para qualquer recurso suportado, o Route 53 ARC aumentará automaticamente a cota do recurso com a cota mais baixa. Isso se aplica somente às cotas (limites). Para obter capacidade, você deve adicionar capacidade adicional conforme necessário para as necessidades do seu aplicativo.

Você também pode configurar uma EventBridge notificação da Amazon para verificações de prontidão, por exemplo, quando o status de qualquer verificação de prontidão mudar para. `NOT`

READY Então, quando uma incompatibilidade de configuração é detectada, EventBridge você recebe uma notificação e você pode tomar medidas corretivas para garantir que as réplicas do aplicativo estejam alinhadas e preparadas para recuperação. Para ter mais informações, consulte Usando o Route 53 ARC com a Amazon EventBridge.

# Verificações de prontidão de recursos de destino do DNS: auditando a prontidão de resiliência

Com as verificações de prontidão de recursos de destino do DNS no Route 53 ARC, você pode auditar a prontidão arquitetônica e de resiliência do seu aplicativo. Esse tipo de verificação de prontidão confere continuamente a arquitetura do seu aplicativo e as políticas de roteamento do Amazon Route 53 para auditar dependências entre zonas e regiões.

Um aplicativo orientado à recuperação tem várias réplicas agrupadas em regiões da AWS ou zonas de disponibilidade, de forma que as réplicas possam falhar independentemente umas das outras. Se seu aplicativo precisar ser ajustado para ser dividido corretamente, o Route 53 ARC sugerirá alterações para atualizar a arquitetura e garantir que ela seja resiliente e esteja pronta para failover.

O Route 53 ARC detecta automaticamente o número e o escopo das células (representando réplicas ou unidades de contenção de falhas) em seu aplicativo e se as células estão em silos por zona de disponibilidade ou por região. Em seguida, o Route 53 ARC identifica e fornece informações sobre os recursos do aplicativo nas células, para determinar se estão corretamente separados em zonas ou regiões. Por exemplo, se você tiver células que têm como escopo zonas específicas, as verificações de prontidão podem monitorar se seus balanceadores de carga e os destinos por trás deles também estão em silos nessas zonas.

Com essas informações, você pode determinar se há alterações que precisam ser feitas para alinhar os recursos em suas células às zonas ou regiões corretas.

Para começar, você cria recursos de destino de DNS para seu aplicativo e conjuntos de recursos e verificações de prontidão para eles. Para ter mais informações, consulte Obter recomendações de arquitetura no Route 53 ARC.

# Criar, atualizar e excluir grupos de recuperação no Route 53 ARC

Um grupo de recuperação representa seu aplicativo no Controlador de recuperação de aplicações do Amazon Route 53. Normalmente, ele consiste em duas ou mais células que são réplicas uma da outra em termos de recursos e funcionalidade, para que você possa fazer o failover de uma para a

outra. Cada célula inclui os nomes de recursos da Amazon (ARNs) para os recursos ativos de uma região da AWS ou zona de disponibilidade. Os recursos podem ser um balanceador de carga do Elastic Load Balancing, um grupo do Auto Scaling ou outros recursos. Uma célula correspondente representando outra zona ou região tem recursos em espera do mesmo tipo que estão em sua célula ativa: um balanceador de carga, um grupo do Auto Scaling e assim por diante.

Uma célula representa réplicas do aplicativo. As verificações de prontidão no Route 53 ARC ajudam você a determinar se o aplicativo está pronto para passar de uma réplica para outra. No entanto, você deve tomar decisões sobre a falha de ou para uma réplica com base em seus sistemas de monitoramento e verificação de integridade. Considere as verificações de prontidão como um serviço complementar a esses sistemas.

A verificação de prontidão audita recursos para determinar a prontidão com base em um conjunto de regras predefinidas para cada tipo de recurso. Depois de criar seu grupo de recuperação com as réplicas, você adiciona verificações de prontidão do Route 53 ARC para os recursos em seu aplicativo, para que o Route 53 ARC garanta que as réplicas tenham a mesma configuração ao longo do tempo.

Tópicos



## Criar grupos de recuperação

As etapas desta seção explicam como criar um grupo de recuperação no console do Route 53 ARC. Para saber como usar operações de API de prontidão de recuperação com o Controlador de recuperação de aplicações do Amazon Route 53, consulte Operações de API de prontidão para recuperação (verificação de prontidão).

Como criar um grupo de recuperação

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Verificação de prontidão.
3. Na página Prontidão de recuperação, escolha Criar e, em seguida, escolha um Grupo de recuperação.
4. Insira um nome para o grupo e escolha Próximo.

5. Escolha Adicionar cluster e, em seguida, Criar.
6. Insira um nome para a célula. Por exemplo, se você tiver uma réplica de aplicativo no Oeste dos EUA (norte da Califórnia), poderá adicionar uma célula chamada `MyApp-us-west-1`.
7. Escolha Adicionar célula e adicione um nome para uma segunda célula. Por exemplo, se você tiver uma réplica no Leste dos EUA (Ohio), poderá adicionar uma célula chamada `MyApp-us-east-2`.
8. Se você quiser adicionar células aninhadas (réplicas em zonas de disponibilidade dentro de regiões), escolha Ação, escolha Adicionar célula aninhada e insira um nome.
9. Depois de adicionar todas as células e células aninhadas às réplicas do seu aplicativo, escolha Avançar.
10. Revise seu grupo de recuperação e escolha Criar grupo de recuperação.

## Atualizar e excluir grupos e células de recuperação

As etapas desta seção explicam como atualizar e excluir um grupo de recuperação e excluir uma célula no console do Route 53 ARC. Para saber como usar operações de API de prontidão de recuperação com o Controlador de recuperação de aplicações do Amazon Route 53, consulte Operações de API de prontidão para recuperação (verificação de prontidão).

Como atualizar ou excluir um grupo de recuperação ou excluir uma célula

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Verificação de prontidão.
3. Na página Prontidão para recuperação, escolha um grupo de recuperação.
4. Para trabalhar com um grupo de recuperação, escolha Ação e depois Editar grupo de recuperação ou Excluir grupo de recuperação.
5. Ao editar um grupo de recuperação, você pode adicionar ou remover células ou células aninhadas.
   - Para adicionar uma célula, escolha Adicionar célula.
   - Para remover uma célula, no rótulo Ação ao lado da célula, escolha Excluir célula.

# Criar e atualizar verificações de prontidão no Route 53 ARC

## Criar e atualizar uma verificação de prontidão

As etapas desta seção explicam como criar uma verificação de prontidão no console do Route 53 ARC. Para saber como usar operações de API de prontidão de recuperação com o Controlador de recuperação de aplicações do Amazon Route 53, consulte Operações de API de prontidão para recuperação (verificação de prontidão).

Para atualizar uma verificação de prontidão, você pode editar o conjunto de recursos para a verificação de prontidão, adicionar ou remover recursos ou alterar o escopo de prontidão de um recurso.

Como criar uma verificação de prontidão

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Verificação de prontidão.
3. Na página Prontidão, escolha Criar e, em seguida, escolha uma Verificação de prontidão.
4. Insira um nome para sua verificação de prontidão, escolha o tipo de recurso que você deseja verificar e, em seguida, escolha Avançar.
5. Adicione um conjunto de recursos para sua verificação de prontidão. Um conjunto de recursos é um grupo de recursos do mesmo tipo em réplicas diferentes. Escolha uma das seguintes opções:

   - Criar uma verificação de prontidão com os recursos em um conjunto de recursos que você já criou.
   - Criar um conjunto de recursos.

   Se você optar por criar um novo conjunto de recursos, insira um nome para ele e escolha Adicionar.
6. Copie e cole nomes de recursos da Amazon (ARNs) um por um para cada recurso que você deseja incluir no conjunto e, em seguida, escolha Avançar.

> **Tip**
>
> Para obter exemplos e mais informações sobre o formato ARN que o Route 53 ARC espera para cada tipo de recurso, consulte Tipos de recursos e formatos ARN no Route 53 ARC.

7. Se quiser, veja as regras de prontidão que serão usadas quando o Route 53 ARC verificar o tipo de recurso que você incluiu nessa verificação de prontidão. Em seguida, escolha Próximo.
8. (Opcional) Em Nome do grupo de recuperação, escolha um grupo ao qual associar a verificação de prontidão. Em seguida, para cada ARN, escolha uma célula (região ou zona de disponibilidade) no menu suspenso em que o recurso está. Se for um recurso no nível do aplicativo, como uma política de roteamento de DNS, escolha Recurso global (sem célula).

   Isso especifica os escopos de prontidão para os recursos na verificação de prontidão.

   > **Important**
   >
   > Embora essa etapa seja opcional, os escopos de prontidão devem ser adicionados para obter informações resumidas de prontidão para seu grupo de recuperação e células. Se você pular essa etapa e não associar a verificação de prontidão aos recursos do seu grupo de recuperação escolhendo escopos de prontidão, o Route 53 ARC não poderá retornar informações resumidas de prontidão para o grupo ou células de recuperação.

9. Escolha Avançar.
10. Revise as informações na página de confirmação e, em seguida, escolha Criar verificação de prontidão.

Como excluir uma verificação de prontidão

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Verificação de prontidão.
3. Escolha uma verificação de prontidão e, em Ações, escolha Excluir.

# Criar e editar conjuntos de recursos

Normalmente, você cria um conjunto de recursos como parte da verificação de prontidão, mas também pode criar um conjunto de recursos separadamente. Você também pode editar um conjunto de recursos para adicionar ou remover recursos. As etapas desta seção explicam como criar ou editar um conjunto de recursos no console do Route 53 ARC. Para saber como usar operações de API de prontidão de recuperação com o Controlador de recuperação de aplicações do Amazon Route 53, consulte Operações de API de prontidão para recuperação (verificação de prontidão).

Como criar um conjunto de recursos.

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/home.
2. Em Controlador de recuperação de aplicações, escolha Conjuntos de recursos.
3. Selecione Create.
4. Insira um nome para o conjunto de recursos e escolha o tipo de recurso a ser incluído no conjunto.
5. Escolha Adicionar e, em seguida, insira o nome de recurso da Amazon (ARN) para o recurso a ser adicionado ao conjunto.
6. Depois de terminar de adicionar recursos, escolha Criar conjunto de recursos.

Como editar um conjunto de recursos

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Verificação de prontidão.
3. Em Conjuntos de recursos, escolha Ação e, em seguida, escolha Editar.
4. Execute um destes procedimentos:
   - Para remover um recurso do conjunto, escolha Remover.
   - Para adicionar um recurso ao conjunto, escolha Adicionar e, em seguida, insira o nome do recurso da Amazon (ARN) para o recurso.
5. Você também pode editar o escopo de prontidão do recurso para associá-lo a uma célula diferente para a verificação de prontidão.
6. Escolha Salvar.

# Monitorar o status de prontidão no Route 53 ARC

Você pode ver a prontidão para seu aplicativo no Controlador de recuperação de aplicações do Amazon Route 53 nos seguintes níveis:

- O nível de verificação de prontidão dos recursos em um conjunto de recursos
- O nível de recurso individual
- O nível da célula (réplica do aplicativo) de todos os recursos em uma região da AWS ou zona de disponibilidade
- O nível do grupo de recuperação para o aplicativo como um todo

Você pode ser notificado sobre alterações no status de prontidão ou pode monitorar as alterações no console do Route 53, ou ainda usando os comandos da CLI do Route 53 ARC.

## Notificação de status de prontidão

Você pode usar EventBridge a Amazon para configurar regras orientadas por eventos para monitorar os recursos ARC do Route 53 e notificá-lo sobre mudanças no status de prontidão. Para ter mais informações, consulte Usando o Route 53 ARC com a Amazon EventBridge.

## Monitorar o status de prontidão no console do Route 53 ARC 53

Esta seção explica como monitorar a prontidão para recuperação no AWS Management Console.

Como monitorar a prontidão de recuperação no console do Route 53 ARC

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Verificação de prontidão.
3. Na página Prontidão, em Grupo de recuperação, visualize o Status de prontidão do grupo de recuperação para cada grupo de recuperação (aplicativo).

   Você também pode visualizar a prontidão de células específicas ou de recursos individuais.

## Monitorar o status de prontidão usando comandos da CLI

Esta seção fornece exemplos de comandos da AWS CLI para ver o status de prontidão do aplicativo e dos recursos em diferentes níveis.

Prontidão para um conjunto de recursos

O status de uma verificação de prontidão que você criou para um conjunto de recursos (um grupo de recursos).

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName
```

Prontidão para um único recurso

Para obter o status de um único recurso em uma verificação de prontidão, incluindo o status de cada regra de prontidão verificada, especifique o nome da verificação de prontidão e o ARN do recurso. Por exemplo: .

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName --resource-arn "arn:aws:dynamodb:us-west-2:111122223333:table/TableName"
```

Prontidão para uma célula

O status de uma única célula, ou seja, uma região ou zona de disponibilidade.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary --cell-name CellName
```

Prontidão para uma aplicação

O status do aplicativo geral, no nível do grupo de recuperação.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary --recovery-group-name RecoveryGroupName
```

# Descrições das regras de prontidão no Route 53 ARC

Esta seção lista as descrições das regras de prontidão para todos os tipos de recursos suportados pelo Controlador de recuperação de aplicações do Amazon Route 53. Para ver uma lista dos tipos de

recursos compatíveis com o Route 53 ARC, consulte Tipos de recursos e formatos ARN no Route 53 ARC.

Você também pode visualizar as descrições das regras de prontidão no console do Route 53 ARC ou usando uma operação de API, fazendo o seguinte:

- Para visualizar as regras de prontidão no console, siga as etapas no procedimento a seguir: Visualizar as regras de prontidão no console.
- Para ver as regras de prontidão usando a API, consulte a ListRulesoperação.

Tópicos



## Regras de prontidão no Route 53 ARC

Esta seção lista o conjunto de regras de prontidão para cada tipo de recurso compatível com o Route 53 ARC.

Ao examinar as descrições das regras, você pode ver que a maioria delas inclui os termos Inspecionar tudo ou Inspecionar um a um. Para entender como esses termos explicam como uma regra funciona no contexto de uma verificação de prontidão e outros detalhes sobre como o Route 53 ARC define o status de prontidão, consulte Como as regras de prontidão determinam o status de prontidão.

### Regras de prontidão

O Route 53 ARC audita os recursos usando as seguintes regras de prontidão.

Etapas da versão 1 do Amazon API Gateway

- ApiGwV1ApiKeyCount: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo número de chaves de API vinculadas.
- ApiGwV1ApiKeySource: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `API Key Source`.
- ApiGwV1BasePath: inspeciona todos os estágios do API Gateway para garantir que eles estejam vinculados ao mesmo caminho básico.

- ApiGwV1BinaryMediaTypes: inspeciona todos os estágios do API Gateway para garantir que sejam compatíveis com os mesmos tipos de mídia binária.
- ApiGwV1CacheClusterEnabled: inspeciona todos os estágios do API Gateway para garantir que todos tenham o `Cache Cluster` habilitado ou que nenhum esteja ativado.
- ApiGwV1CacheClusterSize: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo `Cache Cluster Size`. Se um deles tiver um valor maior, os outros serão marcados como NÃO PRONTO.
- ApiGwV1CacheClusterStatus: inspeciona todos os estágios do API Gateway para garantir que o `Cache Cluster` esteja no estado DISPONÍVEL.
- ApiGwV1DisableExecuteApiEndpoint: inspeciona todos os estágios do API Gateway para garantir que todos os `Execute API Endpoint` tenham sido desativados, ou que nenhum esteja desativado.
- ApiGwV1DomainName: inspeciona todos os estágios do API Gateway para garantir que eles estejam vinculados ao mesmo nome de domínio.
- ApiGwV1EndpointConfiguration: inspeciona todos os estágios do API Gateway para garantir que eles estejam vinculados a um domínio com a mesma configuração de endpoint.
- ApiGwV1EndpointDomainNameStatus: inspeciona todos os estágios do API Gateway para garantir que o nome de domínio ao qual eles estão vinculados esteja no estado DISPONÍVEL.
- ApiGwV1MethodSettings: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Method Settings`.
- ApiGwV1MutualTlsAuthentication: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Mutual TLS Authentication`.
- ApiGwV1Policy: inspeciona todos os estágios do API Gateway para garantir que todos usem políticas de nível de API ou nenhum use.
- ApiGwV1RegionalDomainName: inspeciona todos os estágios do API Gateway para garantir que eles estejam vinculados ao mesmo nome de domínio regional. Nota: essa regra não afeta o status de prontidão.
- ApiGwV1ResourceMethodConfigs: inspeciona todos os estágios do API Gateway para garantir que eles tenham uma hierarquia de recursos semelhante, incluindo as configurações relacionadas.
- ApiGwV1SecurityPolicy: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Security Policy`.
- ApiGwV1Quotas: inspeciona todos os grupos do API Gateway para garantir que estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

- ApiGwV1UsagePlans: inspeciona todos os estágios do API Gateway para garantir que os `Usage Plans` estejam vinculados à mesma configuração.

Etapas da versão 2 do Amazon API Gateway

- ApiGwV2ApiKeySelectionExpression: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `API Key Selection Expression`.
- ApiGwV2ApiMappingSelectionExpression: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `API Mapping Selection Expression`.
- ApiGwV2CorsConfiguration: inspeciona todos os estágios do API Gateway para garantir que eles tenham a mesma configuração relacionada ao CORS.
- ApiGwV2DomainName: inspeciona todos os estágios do API Gateway para garantir que eles estejam vinculados ao mesmo nome de domínio.
- ApiGwV2DomainNameStatus: inspeciona todos os estágios do API Gateway para garantir que o nome de domínio esteja no estado DISPONÍVEL.
- ApiGwV2EndpointType: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Endpoint Type`.
- ApiGwV2Quotas: inspeciona todos os grupos do API Gateway para garantir que estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.
- ApiGwV2MutualTlsAuthentication: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Mutual TLS Authentication`.
- ApiGwV2ProtocolType: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Protocol Type`.
- ApiGwV2RouteConfigs: inspeciona todos os estágios do API Gateway para garantir que eles tenham a mesma hierarquia de rotas com a mesma configuração.
- ApiGwV2RouteSelectionExpression: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Route Selection Expression`.
- ApiGwV2RouteSettings: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Default Route Settings`.
- ApiGwV2SecurityPolicy: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Security Policy`.
- ApiGwV2StageVariables: inspeciona todos os estágios do API Gateway para garantir que todos os `Stage Variables` sejam iguais aos outros estágios.
- ApiGwV2ThrottlingBurstLimit: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Throttling Burst Limit`.

- ApiGwV2ThrottlingRateLimit: inspeciona todos os estágios do API Gateway para garantir que eles tenham o mesmo valor para `Throttling Rate Limit`.

Clusters do Amazon Aurora

- RdsClusterStatus: inspeciona cada cluster do Aurora para garantir que ele tenha um status de `AVAILABLE` ou `BACKING-UP`.
- RdsEngineMode: inspeciona todos os clusters do Aurora para garantir que eles tenham o mesmo valor para `Engine Mode`.
- RdsEngineVersion: inspeciona todos os clusters do Aurora para garantir que eles tenham o mesmo valor para `Major Version`.
- RdsGlobalReplicaLag: inspeciona cada cluster do Aurora para garantir que ele um `Global Replica Lag` de menos de 30 segundos.
- RdsNormalizedCapacity: inspeciona todos os clusters do Aurora para garantir que eles tenham uma capacidade normalizada dentro de 15% do máximo no conjunto de recursos.
- RdsInstanceType: inspeciona todos os clusters do Aurora para garantir que eles tenham os mesmos tipos de instância.
- RdsQuotas: inspeciona todos os clusters do Aurora para garantir que estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

Grupos do Auto Scaling

- AsgMinSizeAndMaxSize: inspeciona todos os grupos do Auto Scaling para que eles tenham os mesmos tamanhos mínimo e máximo.
- AsgAZCount: inspeciona todos os grupos do Auto Scaling para que eles tenham o mesmo número de zonas de disponibilidade.
- AsgInstanceTypes: inspeciona todos os grupos do Auto Scaling para que eles tenham os mesmos tipos de instância. Nota: essa regra não afeta o status de prontidão.
- AsgInstanceSizes: inspeciona todos os grupos do Auto Scaling para garantir que eles tenham os mesmos tamanhos de instância.
- AsgNormalizedCapacity: inspeciona todos os grupos do Auto Scaling para garantir que eles tenham uma capacidade normalizada dentro de 15% do máximo no conjunto de recursos.
- AsgQuotas: inspeciona todos os grupos do Auto Scaling para garantir que estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

CloudWatch alarmes

- CloudWatchAlarmState: inspeciona CloudWatch os alarmes para garantir que cada um não esteja no estado `ALARM` ou`INSUFFICIENT_DATA`.

Gateways do cliente

- CustomerGatewayIpAddress: inspeciona todos os gateways do cliente para garantir que eles tenham o mesmo endereço IP.
- CustomerGatewayState: inspeciona os gateways do cliente para garantir que cada um esteja no estado `AVAILABLE`.
- CustomerGatewayVPNType: inspeciona todos os gateways do cliente para garantir que eles tenham o mesmo tipo de VPN.

DNS target resources

- DnsTargetResourceHostedZoneConfigurationRule: inspeciona todos os recursos de destino do DNS para garantir que eles tenham o mesmo ID de zona hospedada do Amazon Route 53 e que nenhuma zona hospedada seja privada. Nota: essa regra não afeta o status de prontidão.
- DnsTargetResourceRecordSetConfigurationRule: inspeciona todos os recursos de destino do DNS para garantir que eles tenham o mesmo tempo de vida útil do registro de recursos (TTL) e que os TTLs sejam menores ou iguais a 300.
- DnsTargetResourceRoutingRule: inspeciona cada recurso de destino DNS associado a um conjunto de registros de recurso de alias para garantir que ele roteie o tráfego para o nome DNS configurado no recurso de destino. Nota: essa regra não afeta o status de prontidão.
- DnsTargetResourceHealthCheckRule: inspeciona todos os recursos de destino do DNS para garantir que as verificações de integridade sejam associadas aos conjuntos de registros de recursos quando apropriado e não de outra forma. Nota: essa regra não afeta o status de prontidão.

Tabelas do Amazon DynamoDB

- DynamoConfiguration: inspeciona todas as tabelas do DynamoDB para garantir que elas tenham as mesmas chaves, atributos, criptografia do lado do servidor e configurações de streams.
- DynamoTableStatus: inspeciona cada tabela do DynamoDB para garantir que ela tenha o status ATIVO.
- DynamoCapacity: inspeciona todas as tabelas do DynamoDB para garantir que suas capacidades de leitura e gravação provisionadas estejam dentro de 20% das capacidades máximas do conjunto de recursos.
- DynamoPeakRcuWcu: inspeciona cada tabela do DynamoDB para garantir que ela tenha tido um pico de tráfego semelhante ao das outras tabelas, a fim de garantir a capacidade provisionada.

- DynamoGsiPeakRcuWcu: inspeciona cada tabela do DynamoDB para garantir que ela tenha uma capacidade máxima de leitura e gravação semelhante à das outras tabelas, para garantir a capacidade provisionada.
- DynamoGsiConfig: inspeciona todas as tabelas do DynamoDB que têm índices secundários globais para garantir que as tabelas usem o mesmo índice, esquema de chave e projeção.
- DynamoGsiStatus: inspeciona todas as tabelas do DynamoDB que têm índices secundários globais para garantir que tenham um status ATIVO.
- DynamoGsiCapacity: inspeciona todas as tabelas do DynamoDB que têm índices secundários globais para garantir que as tabelas tenham capacidades de leitura e gravação de GSI provisionadas dentro de 20% das capacidades máximas do conjunto de recursos.
- DynamoReplicationLatency: inspeciona todas as tabelas do DynamoDB que são tabelas globais para garantir que elas tenham a mesma latência de replicação.
- DynamoAutoScalingConfiguration: inspeciona todas as tabelas do DynamoDB que têm o Auto Scaling ativado para garantir que elas tenham as mesmas capacidades mínimas, máximas e de destino de leitura e gravação.
- DynamoQuotas: inspeciona todas as tabelas do DynamoDB para garantir que elas estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

Elastic Load Balancing (Classic Load Balancers)

- ElbV1CheckAzCount: inspeciona cada Classic Load Balancer para garantir que ele esteja conectado a apenas uma zona de disponibilidade. Nota: essa regra não afeta o status de prontidão.
- ElbV1AnyInstances: inspeciona todos os Classic Load Balancers para garantir que eles tenham pelo menos uma instância do EC2.
- ElbV1AnyInstancesHealthy: inspeciona todos os Classic Load Balancers para garantir que eles tenham pelo menos uma instância EC2 íntegra.
- ElbV1Scheme: inspeciona todos os Classic Load Balancers para garantir que eles tenham o mesmo esquema de balanceador de carga.
- ElbV1HealthCheckThreshold: inspeciona todos os Classic Load Balancers para garantir que eles tenham o mesmo valor limite de verificação de integridade.
- ElbV1HealthCheckInterval: inspeciona todos os Classic Load Balancers para garantir que eles tenham o mesmo valor de intervalo de verificação de integridade.
- ElbV1CrossZoneRoutingEnabled: inspeciona todos os balanceadores de carga clássicos para garantir que eles tenham o mesmo valor para balanceamento de carga entre zonas (ATIVADO ou DESATIVADO).

- ElbV1AccessLogsEnabledAttribute: inspeciona todos os Classic Load Balancers para garantir que eles tenham o mesmo valor para os logs de acesso (ATIVADO ou DESATIVADO).
- ElbV1ConnectionDrainingEnabledAttribute: inspeciona todos os Classic Load Balancers para garantir que eles tenham o mesmo valor de drenagem de conexão (ATIVADO ou DESATIVADO).
- ElbV1ConnectionDrainingTimeoutAttribute: inspeciona todos os Classic Load Balancers para garantir que eles tenham o mesmo valor de tempo limite de drenagem da conexão.
- ElbV1IdleTimeoutAttribute: inspeciona todos os Classic Load Balancers para garantir que eles tenham o mesmo valor de tempo limite de inatividade.
- ElbV1ProvisionedCapacityLcuCount: inspeciona todos os Classic Load Balancers com uma LCU provisionada maior que 10 para garantir que estejam dentro de 20% da LCU mais alta provisionada no conjunto de recursos.
- ElbV1ProvisionedCapacityStatus: inspeciona o status da capacidade provisionada em cada Classic Load Balancer para garantir que ele não tenha um valor de DISABLED ou PENDING.

Volumes do Amazon EBS

- EbsVolumeEncryption: inspeciona todos os volumes de EBS para garantir que eles tenham o mesmo valor de criptografia (ATIVADO ou DESATIVADO).
- EbsVolumeEncryptionDefault: inspeciona todos os volumes EBS para garantir que eles tenham o mesmo valor de criptografia por padrão (ATIVADO ou DESATIVADO).
- EbsVolumeIops: inspeciona todos os volumes de EBS para garantir que eles tenham as mesmas operações de entrada/saída por segundo (IOPS).
- EbsVolumeKmsKeyId: inspeciona todos os volumes de EBS para garantir que eles tenham o mesmo ID de chave padrão AWS KMS.
- EbsVolumeMultiAttach: inspeciona todos os volumes de EBS para garantir que eles tenham o mesmo valor para conexão múltipla (ATIVADO ou DESATIVADO).
- EbsVolumeQuotas: inspeciona todos os volumes de EBS para garantir que estejam em conformidade com as cotas (limites) definidas pelo Service Quotas.
- EbsVolumeSize: inspeciona todos os volumes de EBS para garantir que tenham o mesmo tamanho legível.
- EbsVolumeState: inspeciona todos os volumes de EBS para garantir que tenham o mesmo estado de volume.
- EbsVolumeType: inspeciona todos os volumes de EBS para garantir que tenham o mesmo tipo de volume.

Funções do AWS Lambda

- LambdaMemorySize: inspeciona todas as funções do Lambda para garantir que elas tenham o mesmo tamanho de memória. Se uma tiver mais memória, as outras serão marcadas `NOT READY`.
- LambdaFunctionTimeout: inspeciona todas as funções do Lambda para garantir que elas tenham o mesmo valor de tempo limite. Se uma tiver um valor maior, as outras serão marcadas `NOT READY`.
- LambdaFunctionRuntime: inspeciona todas as funções do Lambda para garantir que todas tenham o mesmo runtime.
- LambdaFunctionReservedConcurrentExecutions: inspeciona todas as funções do Lambda para garantir que todas tenham o mesmo valor para `Reserved Concurrent Executions`. Se uma tiver um valor maior, as outras serão marcadas `NOT READY`.
- LambdaFunctionDeadLetterConfig: inspeciona todas as funções do Lambda para garantir que todas tenham um `Dead Letter Config` definido, ou que nenhuma delas tenha.
- LambdaFunctionProvisionedConcurrencyConfig: inspeciona todas as funções do Lambda para garantir que elas tenham o mesmo valor para `Provisioned Concurrency`.
- LambdaFunctionSecurityGroupCount: inspeciona todas as funções do Lambda para garantir que elas tenham o mesmo valor para `Security Groups`.
- LambdaFunctionSubnetIdCount: inspeciona todas as funções do Lambda para garantir que elas tenham o mesmo valor para `Subnet Ids`.
- LambdaFunctionEventSourceMappingMatch: inspeciona todas as funções do Lambda para garantir que todas as propriedades de `Event Source Mapping` escolhidas correspondam entre elas.
- LambdaFunctionLimitsRule: inspeciona todas as funções do Lambda para garantir que elas estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

Network Load Balancers e Application Load Balancers

- ElbV2CheckAzCount: inspeciona cada Network Load Balancer para garantir que ele esteja conectado somente a uma zona de disponibilidade. Nota: essa regra não afeta o status de prontidão.
- ElbV2TargetGroupsCanServeTraffic: inspeciona cada Network Load Balancer e Application Load Balancer para garantir que eles tenham pelo menos uma instância íntegra no Amazon EC2.
- ElbV2State: inspeciona cada Network Load Balancer e Application Load Balancer para garantir que estejam no estado `ACTIVE`.

- ElbV2IpAddressType: inspeciona todos os Network Load Balancers e Application Load Balancers para garantir que eles tenham os mesmos tipos de endereço IP.
- ElbV2Scheme: inspeciona todos os Network Load Balancers e Application Load Balancers para garantir que eles tenham o mesmo esquema.
- ElbV2Type: inspeciona todos os Network Load Balancers e Application Load Balancers para garantir que eles tenham o mesmo tipo.
- ElbV2S3LogsEnabled: inspeciona todos os Network Load Balancers e Application Load Balancers para garantir que eles tenham o mesmo valor para os logs de acesso ao servidor Amazon S3 (ATIVADOS ou DESATIVADOS).
- ElbV2DeletionProtection: inspeciona todos os Network Load Balancers e Application Load Balancers para garantir que eles tenham o mesmo valor de proteção contra exclusão (ATIVADO ou DESATIVADO).
- ElbV2IdleTimeoutSeconds: inspeciona todos os Network Load Balancers e Application Load Balancers para garantir que eles tenham o mesmo valor para segundos de tempo ocioso.
- ElbV2HttpDropInvalidHeaders: inspeciona todos os Network Load Balancers e Application Load Balancers para garantir que eles tenham o mesmo valor para cabeçalhos inválidos de eliminação de HTTP.
- ElbV2Http2Enabled: inspeciona todos os Network Load Balancers e Application Load Balancers para garantir que eles tenham o mesmo valor para HTTP2 (ATIVADO ou DESATIVADO).
- ElbV2CrossZoneEnabled: inspeciona todos os Network Load Balancers and Application Load Balancers para garantir que eles tenham o mesmo valor para balanceamento de carga entre zonas (ATIVADO ou DESATIVADO).
- ElbV2ProvisionedCapacityLcuCount: inspeciona todos os Network Load Balancers e Application Load Balancers com uma LCU provisionada maior que 10 para garantir que estejam dentro de 20% da LCU mais alta provisionada no conjunto de recursos.
- ElbV2ProvisionedCapacityEnabled: inspeciona o status da capacidade provisionada de todos os Network Load Balancers e Application Load Balancers para garantir que ela não tenha um valor de DISABLED ou PENDING.

Clusters do Amazon MSK

- MskClusterClientSubnet: inspeciona cada cluster do MSK para garantir que ele tenha somente duas ou somente três sub-redes de clientes.
- MskClusterInstanceType: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo tipo de instância do Amazon EC2.

- MskClusterSecurityGroups: inspeciona todos os clusters do MSK para garantir que eles tenham os mesmos grupos de segurança.
- MskClusterStorageInfo: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo tamanho de volume de armazenamento do EBS. Se um tiver um valor maior, os outros serão marcados como NÃO PRONTO.
- MskClusterACMCertificate: inspeciona todos os clusters do MSK para garantir que eles tenham a mesma lista de ARNs de certificados de autorização do cliente.
- MskClusterServerProperties: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Current Broker Software Info`.
- MskClusterKafkaVersion: inspeciona todos os clusters do MSK para garantir que eles tenham a mesma versão do Kafka.
- MskClusterEncryptionInTransitInCluster: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Encryption In Transit In Cluster`.
- MskClusterEncryptionInClientBroker: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Encryption In Transit Client Broker`.
- MskClusterEnhancedMonitoring: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Enhanced Monitoring`.
- MskClusterOpenMonitoringInJmx: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Open Monitoring JMX Exporter`.
- MskClusterOpenMonitoringInNode: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Open Monitoring Not Exporter.`.
- MskClusterLoggingInS3: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Is Logging in S3`.
- MskClusterLoggingInFirehose: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Is Logging In Firehose`.
- MskClusterLoggingInCloudWatch: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Is Logging Available In CloudWatch Logs`.
- MskClusterNumberOfBrokerNodes: inspeciona todos os clusters do MSK para garantir que eles tenham o mesmo valor para `Number of Broker Nodes`. Se um tiver um valor maior, os outros serão marcados como NÃO PRONTO.
- MskClusterState: inspeciona cada cluster do MSK para garantir que ele esteja em um estado ATIVO.

- MskClusterLimitsRule: inspeciona todas as funções do Lambda para garantir que elas estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

Verificações de integridade do Amazon Route 53

- R53HealthCheckType: inspeciona cada verificação de integridade do Route 53 para garantir que ela não seja do tipo CALCULATED e que todas as verificações sejam do mesmo tipo.
- R53HealthCheckDisabled: inspeciona cada verificação de integridade do Route 53 para garantir que ela não tenha um estado DESATIVADO.
- R53HealthCheckStatus: inspeciona cada verificação de integridade do Route 53 para garantir que ela tenha um status de SUCESSO.
- R53HealthCheckRequestInterval: inspeciona todas as verificações de integridade do Route 53 para garantir que todas tenham o mesmo valor para `Request Interval`.
- R53HealthCheckFailureThreshold: inspeciona todas as verificações de integridade do Route 53 para garantir que todas tenham o mesmo valor para `Failure Threshold.`.
- R53HealthCheckEnableSNI: inspeciona todas as verificações de integridade do Route 53 para garantir que todas tenham o mesmo valor para `Enable SNI.`
- R53HealthCheckSearchString: inspeciona todas as verificações de integridade do Route 53 para garantir que todas tenham o mesmo valor para `Search String.`.
- R53HealthCheckRegions: inspeciona todas as verificações de integridade do Route 53 para garantir que todas tenham a mesma lista de regiões da AWS.
- R53HealthCheckMeasureLatency: inspeciona todas as verificações de integridade do Route 53 para garantir que todas tenham o mesmo valor para `Measure Latency`.
- R53HealthCheckInsufficientDataHealthStatus: inspeciona todas as verificações de integridade do Route 53 para garantir que todas tenham o mesmo valor para `Insufficient Data Health Status`.
- R53HealthCheckInverted: inspeciona todas as verificações de integridade do Route 53 para garantir que todas estejam invertidas, ou todas estejam não invertidas.
- R53HealthCheckResourcePath: inspeciona todas as verificações de integridade do Route 53 para garantir que todas tenham o mesmo valor para `Resource Path`.
- R53HealthCheckCloudWatchAlarm: inspeciona todas as verificações de saúde do Route 53 para garantir que os CloudWatch alarmes associados a elas tenham as mesmas configurações e configurações.

Assinaturas do Amazon SNS

- SnsSubscriptionProtocol: inspeciona todas as assinaturas do SNS para garantir que elas tenham o mesmo protocolo.
- SnsSubscriptionSqsLambdaEndpoint: inspeciona todas as assinaturas do SNS que têm endpoints Lambda ou SQS para garantir que tenham endpoints diferentes.
- SnsSubscriptionNonAwsEndpoint: inspeciona todas as assinaturas do SNS que têm um tipo de endpoint sem serviço da AWS, por exemplo, e-mail, para garantir que as assinaturas tenham o mesmo endpoint.
- SnsSubscriptionPendingConfirmation: inspeciona todas as assinaturas do SNS para garantir que elas tenham o mesmo valor para “Confirmações pendentes”.
- SnsSubscriptionDeliveryPolicy: inspeciona todas as assinaturas do SNS que usam HTTP/S para garantir que elas tenham o mesmo valor para “Período de entrega efetivo”.
- SnsSubscriptionRawMessageDelivery: inspeciona todas as assinaturas do SNS para garantir que elas tenham o mesmo valor para “Entrega de mensagens brutas”.
- SnsSubscriptionFilter: inspeciona todas as assinaturas do SNS para garantir que elas tenham o mesmo valor para “Política de filtro”.
- SnsSubscriptionRedrivePolicy: inspeciona todas as assinaturas do SNS para garantir que elas tenham o mesmo valor para a “Política de redirecionamento”.
- SnsSubscriptionEndpointEnabled: inspeciona todas as assinaturas do SNS para garantir que elas tenham o mesmo valor para “Endpoint habilitado”.
- SnsSubscriptionLambdaEndpointValid: inspeciona todas as assinaturas do SNS que têm endpoints Lambda para garantir que tenham endpoints Lambda válidos.
- SnsSubscriptionSqsEndpointValidRule: inspeciona todas as assinaturas do SNS que usam endpoints do SQS para garantir que tenham pontos finais do SQS válidos.
- SnsSubscriptionQuotas: inspeciona todas as assinaturas do SNS para garantir que elas estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

Tópicos do Amazon SNS

- SnsTopicDisplayName: inspeciona todos os tópicos do SNS para garantir que eles tenham o mesmo valor para `Display Name`.
- SnsTopicDeliveryPolicy: inspeciona todos os tópicos do SNS que têm assinantes HTTPS para garantir que eles tenham os mesmos `EffectiveDeliveryPolicy`.
- SnsTopicSubscription: inspeciona todos os tópicos do SNS para garantir que eles tenham o mesmo número de assinantes para cada um de seus protocolos.

- SnsTopicAwsKmsKey: inspeciona todos os tópicos do SNS para garantir que todos os tópicos ou nenhum deles tenham uma chave AWS KMS.
- SnsTopicQuotas: inspeciona todos os tópicos do SNS para garantir que estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

Filas do Amazon SQS

- SqsQueueType: inspeciona todas as filas do SQS para garantir que todas tenham o mesmo valor para `Type`.
- SqsQueueDelaySeconds: inspeciona todas as filas do SQS para garantir que todas tenham o mesmo valor para `Delay Seconds`.
- SqsQueueMaximumMessageSize: inspeciona todas as filas do SQS para garantir que todas tenham o mesmo valor para `Maximum Message Size`.
- SqsQueueMessageRetentionPeriod: inspeciona todas as filas do SQS para garantir que todas tenham o mesmo valor para `Message Retention Period`.
- SqsQueueReceiveMessageWaitTimeSeconds: inspeciona todas as filas do SQS para garantir que todas tenham o mesmo valor para `Receive Message Wait Time Seconds`.
- SqsQueueRedrivePolicyMaxReceiveCount: inspeciona todas as filas do SQS para garantir que todas tenham o mesmo valor para `Redrive Policy Max Receive Count`.
- SqsQueueVisibilityTimeout: inspeciona todas as filas do SQS para garantir que todas tenham o mesmo valor para `Visibility Timeout`.
- SqsQueueContentBasedDeduplication: inspeciona todas as filas do SQS para garantir que todas tenham o mesmo valor para `Content-Based Deduplication`.
- SqsQueueQuotas: inspeciona todas as filas do SQS para garantir que elas estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

Amazon VPCs

- VpcCidrBlock: inspeciona todas as VPCs para garantir que todas tenham o mesmo valor para o tamanho da rede de blocos CIDR.
- VpcCidrBlocksSameProtocolVersion: inspeciona todas as VPCs que têm os mesmos blocos CIDR para garantir que tenham o mesmo valor para o número de versão do Internet Stream Protocol.
- VpcCidrBlocksStateInAssociationSets: inspeciona todos os conjuntos de associação de blocos CIDR para todas as VPCs para garantir que todas tenham blocos CIDR em um estado `ASSOCIATED`.

- VpcIpv6CidrBlocksStateInAssociationSets: inspeciona todos os conjuntos de associação de blocos CIDR para todas as VPCs para garantir que todas tenham blocos CIDR com o mesmo número de endereços.
- VpcCidrBlocksInAssociationSets: inspeciona todos os conjuntos de associação de blocos CIDR para todas as VPCs para garantir que todas tenham o mesmo tamanho.
- VpcIpv6CidrBlocksInAssociationSets: inspeciona todos os conjuntos de associação de blocos CIDR IPv6 para todas as VPCs para garantir que elas tenham o mesmo tamanho.
- VpcState: inspeciona cada VPC para garantir que ela esteja em estado `AVAILABLE`.
- VpcInstanceTenancy: inspeciona todas as VPCs para garantir que todas tenham o mesmo valor para `Instance Tenancy`.
- VpcIsDefault: inspeciona todas as VPCs para garantir que elas tenham o mesmo valor para `Is Default.`.
- VpcSubnetState: inspeciona cada sub-rede VPC para garantir que ela esteja em um estado DISPONÍVEL.
- VpcSubnetAvailableIpAddressCount: inspeciona cada sub-rede VPC para garantir que ela tenha uma contagem de endereços IP disponível maior que zero.
- VpcSubnetCount: inspeciona todas as sub-redes VPC para garantir que elas tenham o mesmo número de sub-redes.
- VpcQuotas: inspeciona todas as sub-redes VPC para garantir que elas estejam em conformidade com as cotas (limites) gerenciadas pelo Service Quotas.

Conexões do AWS VPN

- VpnConnectionsRouteCount: inspeciona todas as conexões VPN para garantir que elas tenham pelo menos uma rota e também o mesmo número de rotas.
- VpnConnectionsEnableAcceleration: inspeciona todas as conexões VPN para garantir que elas tenham o mesmo valor para `Enable Accelerations`.
- VpnConnectionsStaticRoutesOnly: inspeciona todas as conexões VPN para garantir que elas tenham o mesmo valor para `Static Routes Only.`.
- VpnConnectionsCategory: inspeciona todas as conexões VPN para garantir que elas tenham uma categoria de `VPN`.
- VpnConnectionsCustomerConfiguration: inspeciona todas as conexões VPN para garantir que elas tenham o mesmo valor para `Customer Gateway Configuration`.
- VpnConnectionsCustomerGatewayId: inspeciona cada conexão VPN para garantir que ela tenha um gateway do cliente conectado.

- VpnConnectionsRoutesState: inspeciona todas as conexões VPN para garantir que elas estejam em um estado `AVAILABLE`.
- VpnConnectionsVgwTelemetryStatus: inspeciona cada conexão VPN para garantir que ela tenha um status VGW de `UP`.
- VpnConnectionsVgwTelemetryIpAddress: inspeciona cada conexão VPN para garantir que ela tenha um endereço IP externo diferente para cada telemetria VGW.
- VpnConnectionsTunnelOptions: inspeciona todas as conexões VPN para garantir que elas tenham as mesmas opções de túnel.
- VpnConnectionsRoutesCidr: inspeciona todas as conexões VPN para garantir que elas tenham os mesmos blocos CIDR de destino.
- VpnConnectionsInstanceType: inspeciona todas as conexões VPN para garantir que elas tenham as mesmas `Instance Type`.

AWS VPNGateways do

- VpnGatewayState: inspeciona todos os gateways de VPN para garantir que eles estejam em um estado DISPONÍVEL.
- VpnGatewayAsn: inspeciona todos os gateways de VPN para garantir que eles tenham o mesmo ASN.
- VpnGatewayType: inspeciona todos os gateways de VPN para garantir que eles tenham o mesmo tipo.
- VpnGatewayAttachment: inspeciona todos os gateways de VPN para garantir que eles tenham as mesmas configurações de anexo.

## Visualizar as regras de prontidão no console

Você pode ver as regras de prontidão no AWS Management Console, listadas por tipo de recurso.

Como visualizar as regras de prontidão no console

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Verificação de prontidão.
3. Em Tipo de recurso, escolha o tipo de recurso para o qual você deseja ver as regras.

# Tipos de recursos e formatos ARN no Route 53 ARC

Ao criar um conjunto de recursos no Controlador de recuperação de aplicações do Amazon Route 53, você especifica o tipo de recurso a ser incluído no conjunto e os nomes dos recursos da Amazon (ARNs) para cada um. O Route 53 ARC espera um formato ARN específico para cada tipo de recurso. Esta seção lista os tipos de recursos suportados pelo Route 53 ARC e os formatos ARN associados a cada um.

Os formatos específicos dependem do recurso. Para usar um ARN, substitua o texto em *itálico* pelas informações específicas do recurso.

> **Note**
>
> Lembre-se de que o formato ARN que o Route 53 ARC exige para os recursos pode ser diferente do formato ARN que o próprio serviço exige. Por exemplo, os formatos ARN descritos nas seções Tipo de recurso para cada serviço na Referência de autorização de serviço podem não incluir a ID da Conta da AWS ou outras informações que o Route 53 ARC precisa para oferecer suporte aos recursos do serviço.

AWS::ApiGateway::Stage

Um estágio do Amazon API Gateway versão 1.

- Formato ARN: `arn:`*`partition`*`:apigateway:`*`region`*`:`*`account`*`:/restapis/`*`api-id`*`/stages/`*`stage-name`*

  Exemplo: `arn:aws:apigateway:us-east-1:111122223333:/restapis/123456789/stages/ExampleStage`

  Para obter mais informações, consulte Referência da API Gateway do nome do recurso da Amazon (ARN).

AWS::ApiGatewayV2::Stage

Um estágio do Amazon API Gateway versão 2.

- Formato ARN: `arn:`*`partition`*`:apigateway:`*`region`*`:`*`account`*`:/apis/`*`api-id`*`/stages/`*`stage-name`*

  Exemplo: `arn:aws:apigateway:us-east-1:111122223333:/apis/123456789/stages/ExampleStage`

Para obter mais informações, consulte Referência da API Gateway do nome do recurso da Amazon (ARN).

AWS::CloudWatch::Alarm

Um CloudWatch alarme da Amazon.

- Formato ARN: `arn:partition:cloudwatch:region:account:alarm:alarm-name`

  Exemplo: `arn:aws:cloudwatch:us-west-2:111122223333:alarm:test-alarm-1`

  Para obter mais informações, consulte Tipos de recursos definidos pela Amazon CloudWatch.

AWS::DynamoDB::Table

Uma tabela do Amazon DynamoDB

- Formato ARN: `arn:partition:dynamodb:region:account:table/table-name`

  Exemplo: `arn:aws:dynamodb:us-west-2:111122223333:table/BigTable`

  Para mais informações, consulte Recursos e operações do DynamoDB.

AWS::EC2::CustomerGateway

Um dispositivo de gateway do cliente

- Formato ARN: `arn:partition:ec2:region:account:customer-gateway/CustomerGatewayId`

  Exemplo: `arn:aws:ec2:us-west-2:111122223333:customer-gateway/vcg-123456789`

  Para obter mais informações, consulte Tipos de recursos definidos pelo Amazon EC2.

AWS::EC2::Volume

Um volume do Amazon EBS

- Formato ARN: `arn:partition:ec2:region:account:volume/VolumeId`

  Exemplo: `arn:aws:ec2:us-west-2:111122223333:volume/volume-of-cylinder-is-pi`

  Para obter mais informações, consulte Referência da API Gateway do nome do recurso da Amazon (ARN).

AWS::ElasticLoadBalancing::LoadBalancer

Um Classic Load Balancer.

- Formato ARN: `arn:partition:elasticloadbalancing:region:account:loadbalancer/LoadBalancerN`

  Exemplo: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/123456789abcbdeCLB`

  Para obter mais informações, consulte Recursos do Elastic Load Balancing.

AWS::ElasticLoadBalancingV2::LoadBalancer

Um Application Load Balancer ou um Network Load Balancer.

- Formato ARN para o Network Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Exemplo de Network Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdeNLB`
- Formato ARN para o Application Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/app/LoadBalancerName`

  Exemplo de Application Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/app/sandbox-alb/123456789acbdeALB`

  Para obter mais informações, consulte Recursos do Elastic Load Balancing.

AWS::Lambda::Function

Uma função do AWS Lambda.

- Formato ARN: `arn:partition:lambda:region:account:function:FunctionName`

  Exemplo: `arn:aws:lambda:us-west-2:111122223333:function:my-function`

  Para mais informações, consulte Recursos e condições para ações do Lambda.

AWS::MSK::Cluster

Um cluster do Amazon MSK.

- Formato ARN: `arn:partition:kafka:region:account:cluster/ClusterName/UUID`

Exemplo: `arn:aws:kafka:us-east-1:111122223333:cluster/demo-cluster-1/123456-1111-2222-3333`

Para mais informações, consulte Tipos de recursos definidos pelo Amazon Managed Streaming for Apache Kafka.

AWS::RDS::DBCluster

Um cluster do Aurora DB

- Formato ARN: `arn:`*`partition`*`:rds:`*`region`*`:`*`account`*`:cluster:`*`DbClusterInstanceName`*

  Exemplo: `arn:aws:rds:us-west-2:111122223333:cluster:database-1`

  Para mais informações, consulte Trabalhar com nomes do recurso da Amazon (ARNs) no Amazon RDS.

AWS::Route53::HealthCheck

Uma verificação de integridade do Amazon Route 53

- Formato ARN: `arn:`*`partition`*`:route53:::healthcheck/`*`Id`*

  Exemplo: `arn:aws:route53:::healthcheck/123456-1111-2222-3333`

AWS::SQS::Queue

Uma fila do Amazon SQS.

- Formato ARN: `arn:`*`partition`*`:sqs:`*`region`*`:`*`account`*`:`*`QueueName`*

  Exemplo: `arn:aws:sqs:us-west-2:111122223333:StandardQueue`

  Para obter mais informações, consulte Recursos e operações do Amazon Simple Queue Service.

AWS::SNS::Topic

Um tópico do Amazon SNS.

- Formato ARN: `arn:`*`partition`*`:sns:`*`region`*`:`*`account`*`:`*`TopicName`*

  Exemplo: `arn:aws:sns:us-west-2:111122223333:TopicName`

  Para obter mais informações, consulte Formato ARN do recurso do Amazon SNS.

AWS::SNS::Subscription

Uma assinatura do Amazon SNS.

- Formato ARN: `arn:partition:sns:region:account:TopicName:SubscriptionId`

  Exemplo: `arn:aws:sns:us-west-2:111122223333:TopicName:12345678901234567890`

AWS::EC2::VPC

Uma nuvem privada virtual (VPC).

- Formato ARN: `arn:partition:ec2:region:account:vpc/VpcId`

  Exemplo: `arn:aws:ec2:us-west-2:111122223333:vpc/vpc-123456789`

  Para obter mais informações, consulte Recursos da VPC.

AWS::EC2::VPNConnection

Uma conexão de rede privada virtual (VPN).

- Formato ARN: `arn:partition:ec2:region:account:vpn-connection/VpnConnectionId`

  Exemplo: `arn:aws:ec2:us-west-2:111122223333:vpn-connection/vpn-123456789`

  Para obter mais informações, consulte Tipos de recursos definidos pelo Amazon EC2.

AWS::EC2::VPNGateway

Um gateway de rede privada virtual (VPN).

- Formato ARN: `arn:partition:ec2:region:account:vpn-gateway/VpnGatewayId`

  Exemplo: `arn:aws:ec2:us-west-2:111122223333:vpn-gateway/vgw-123456789acbdefgh`

  Para obter mais informações, consulte Tipos de recursos definidos pelo Amazon EC2.

AWS::Route53RecoveryReadiness::DNSTargetResource

Um recurso de destino de DNS para verificações de prontidão inclui o tipo de registro DNS, nome de domínio, ARN da zona hospedada do Route 53 e ARN do Network Load Balancer ou ID do conjunto de registros do Route 53.

- Formato ARN para zona hospedada: `arn:partition:route53::account:hostedzone/Id`

  Exemplo de uma zona hospedada: `arn:aws:route53::111122223333:hostedzone/abcHostedZone`

  Obs.: você deve incluir o ID da conta nos ARNs da zona hospedada, conforme especificado aqui. O ID da conta é necessário para que o Route 53 ARC possa pesquisar o recurso. O formato é intencionalmente diferente do formato ARN exigido pelo Amazon Route 53, descrito em Tipos de recursos na Referência de autorização do serviço.

- Formato ARN para o Network Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Exemplo de Network Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdefgh`

  Para obter mais informações, consulte Recursos do Elastic Load Balancing.

# Obter recomendações de arquitetura no Route 53 ARC

Se você já tem um aplicativo, o Controlador de recuperação de aplicações do Amazon Route 53 pode avaliar a arquitetura dele e as políticas de roteamento e fornecer recomendações para modificar o design a fim de melhorar a resiliência de recuperação do aplicativo. Depois de criar um grupo de recuperação no Route 53 ARC que represente seu aplicativo, siga as etapas nesta seção para obter recomendações para a arquitetura do seu aplicativo.

Recomendamos que você especifique um recurso de destino para o recurso de destino DNS do seu grupo de recuperação, caso ainda não tenha especificado um, para receber recomendações mais detalhadas. Quando você dá informações adicionais, o Route 53 ARC pode fornecer recomendações melhores. Por exemplo, se você inserir um registro de recurso do Amazon Route 53 ou um Network Load Balancer como recurso de destino, o Route 53 ARC poderá fornecer informações sobre se você criou o número ideal de células para seu grupo de recuperação.

Observe o seguinte para os recursos de destino do DNS:

- Especifique somente um registro de recurso do Route 53 ou Network Load Balancer para um recurso de destino.

- Crie somente um recurso de destino DNS para cada grupo de recuperação.
- Recomendado: crie um recurso de destino DNS para cada célula.
- Agrupe os recursos de destino do DNS em um conjunto de recursos com uma verificação de prontidão.

O procedimento a seguir explica como criar recursos de destino de DNS e obter recomendações de arquitetura para seu aplicativo.

Como obter recomendações para atualizar sua arquitetura

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Verificação de prontidão.
3. Em Nome do grupo de recuperação, escolha o grupo de recuperação que representa seu aplicativo.
4. Na página de Detalhes do grupo de recuperação, no menu Ação, escolha Obter recomendações de arquitetura para esse grupo de recuperação.
5. Se você ainda não criou uma verificação de prontidão de recursos de destino de DNS, crie uma para que o Route 53 ARC dê recomendações de arquitetura. Escolha Criar um recurso de destino DNS.

   Para obter mais informações sobre recursos do DNS de destino, consulte Componentes da verificação de prontidão .
6. Para criar um conjunto de recursos para um recurso de destino de DNS, você cria uma verificação de prontidão. Insira um nome para a verificação de prontidão e, em seguida, para o tipo, escolha Recurso de destino DNS.
7. Insira um nome para o conjunto de recursos.
8. Insira os atributos do seu aplicativo, incluindo o nome DNS, o ARN da zona hospedada e o ID do conjunto de registros.

> **Tip**
>
> Para ver o formato de um ARN de zona hospedada, consulte Formato de ARN para zona hospedada em Tipos de recursos e formatos ARN no Route 53 ARC.

Opcionalmente, mas altamente recomendado: escolha Adicionar atributo opcional e forneça um ARN do Network Load Balancer ou o registro de recursos do Route 53 do seu domínio.

9. (Opcional) Na Configuração do grupo de recuperação, escolha uma célula para seu recurso de destino de DNS para definir o escopo de prontidão.
10. Escolha Criar compartilhamento de recursos.
11. Na página de detalhes do Grupo de recuperação, escolha Obter recomendações de arquitetura. O Route 53 ARC exibe um conjunto de recomendações na página.

Revise a lista de recomendações. Depois, você pode decidir se e como fazer alterações para melhorar a resiliência de recuperação do seu aplicativo.

## Criar autorizações entre contas no Route 53 ARC

Você pode ter seus recursos distribuídos em várias contas da AWS, o que pode dificultar a obtenção de uma visão abrangente da integridade do aplicativo e das informações necessárias para tomar decisões rápidas. Para simplificar isso no Controlador de recuperação de aplicações do Amazon Route 53, você pode usar a Autorização entre contas.

A autorização entre contas no Route 53 ARC funciona com o atributo de verificação de prontidão. Com a autorização entre contas, você pode usar uma conta da AWS central para monitorar seus recursos localizados em várias contas da AWS. Em cada conta com recursos que deseja monitorar, você autoriza a conta central a ter acesso a eles. Em seguida, a conta central pode criar verificações de prontidão para os recursos em todas as contas e, a partir da conta central, você pode monitorar a prontidão para o failover.

> **Note**
>
> A configuração de autorização entre contas não está disponível no console. Em vez disso, use as operações da API do Route 53 ARC para configurar e trabalhar com a autorização entre contas. Para começar, esta seção fornece exemplos de comandos da AWS CLI.

Digamos que um aplicativo tenha uma conta com recursos na região Oeste dos EUA (Oregon, us-west-2) e que também tenha recursos que você gostaria de monitorar na região Leste dos EUA

(N. da Virgínia, us-east-1). O Route 53 ARC pode permitir que você monitore os dois conjuntos de recursos de uma conta, us-west-2, usando a autorização entre contas.

Por exemplo, digamos que você tem as seguintes contas da AWS:

- Conta do Oeste dos EUA: 999999999999
- Conta do Leste dos EUA: 1111111111

Na conta us-east-1 (111111111111), podemos habilitar a autorização entre contas para permitir o acesso pela conta us-west-2 (999999999999) especificando o nome do recurso da Amazon (ARN) para o usuário (raiz) na conta do IAM us-west-2: `arn:aws:iam::999999999999:root`. Depois de criar a autorização, a conta us-west-2 pode adicionar recursos de propriedade de us-east-1 aos conjuntos de recursos e criar verificações de prontidão para execução nos conjuntos.

O exemplo a seguir ilustra a configuração da autorização entre contas. Você deve habilitar a autorização entre contas em cada conta adicional com recursos da AWS que você deseja adicionar e monitorar no Route 53 ARC.

> **Note**
>
> O Route 53 ARC é um serviço global que oferece suporte a endpoints em várias regiões da AWS, mas você deve especificar a região Oeste dos EUA (Oregon), ou seja, especificar o parâmetro `--region us-west-2`, na maioria dos comandos da CLI do Route 53 ARC.

O comando da AWS CLI a seguir mostra como configurar a autorização entre contas neste exemplo:

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    create-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

Para desativar essa autorização, faça o seguinte:

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    delete-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

Para verificar em uma conta específica todas as contas para as quais você forneceu autorização entre contas, use o comando `list-cross-account-authorizations`. Observe que, no momento, não será possível fazer o check-in na outra direção. Ou seja, não há uma operação de API para usar com um perfil de conta para listar todas as contas autorizadas entre contas para adicionar e monitorar recursos.

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-account \
    list-cross-account-authorizations
```

```
{
    "CrossAccountAuthorizations": [
        "arn:aws:iam::999999999999:root"
    ]
}
```

# Controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53

Para fazer o failover do tráfego para réplicas de aplicativos no Controlador de recuperação de aplicações do Amazon Route 53, use controles de roteamento integrados a um tipo específico de verificação de integridade no Amazon Route 53. Os controles de roteamento são simples interruptores liga-desliga que permitem que você alterne o tráfego do seu cliente de uma réplica para outra. O redirecionamento do tráfego é realizado por meio de verificações de integridade do controle de roteamento que são configuradas com os registros DNS do Amazon Route 53. Por exemplo, registros de failover de DNS, associados a nomes de domínio que estão na frente das réplicas de seu aplicativo. Este capítulo explica como o controle de roteamento funciona, como configurar componentes de controle de roteamento e como usá-los para redirecionar o tráfego para o failover.

Os componentes de controle de roteamento no Route 53 ARC são: clusters, painéis de controle, controles de roteamento e verificações de integridade do controle de roteamento. Todos os controles de roteamento são agrupados em painéis de controle. Você pode agrupá-los no painel de controle padrão que o Route 53 ARC cria para seu cluster ou criar seus próprios painéis personalizados. É necessário criar um cluster antes de criar um painel de controle ou um controle de roteamento. Cada cluster no Route 53 ARC é um plano de dados de endpoints em cinco Regiões da AWS.

Depois de criar controles de roteamento e verificações de integridade do controle de roteamento, você pode criar regras de segurança para ajudar a evitar efeitos colaterais não intencionais da automação de recuperação. Você pode atualizar os estados de controle de roteamento para redirecionar o tráfego, individualmente ou em lotes, usando as ações da API na AWS CLI ou (recomendado) ou usando o AWS Management Console.

Este capítulo explica como os controles de roteamento funcionam, como criá-los e usá-los para redirecionar o tráfego para seu aplicativo.

> **Important**
>
> Para saber como se preparar para usar o Route 53 ARC para redirecionar o tráfego como parte de um plano de failover para seu aplicativo em um cenário de desastre, consulte Práticas recomendadas para o Controlador de recuperação de aplicações do Amazon Route 53.

Tópicos



# Sobre o controle de roteamento

O controle de roteamento redireciona o tráfego usando verificações de integridade no Amazon Route 53 que são configuradas com registros DNS associados ao atributo de nível superior das células em seu grupo de recuperação, como um balanceador de carga do Elastic Load Balancing. Você pode redirecionar o tráfego de uma célula para outra, por exemplo, atualizando um estado de controle de roteamento para `Off` (para interromper o fluxo de tráfego para uma célula) e atualizando outro estado de controle de roteamento para On (para iniciar o fluxo de tráfego para outra). O processo que altera o fluxo de tráfego é a verificação de integridade do Route 53 associada ao controle de roteamento, depois que o Route 53 ARC o atualiza para defini-lo como íntegro ou não íntegro com base no estado de controle de roteamento correspondente.

Os controles de roteamento oferecem suporte ao failover em qualquer serviço da AWS que tenha um endpoint de DNS. Você pode atualizar os estados de controle de roteamento para permitir o failover do tráfego para recuperação de desastres ou ao detectar quedas de latência em seu aplicativo ou outros problemas.

Você também pode configurar regras de segurança no Route 53 ARC para garantir que o redirecionamento do tráfego usando controles de roteamento não prejudique a disponibilidade. Para ter mais informações, consulte Criação de regras de segurança no Route 53 ARC .

É importante observar que os controles de roteamento não são, em si, verificações de integridade que monitoram a integridade subjacente dos endpoints. Por exemplo, ao contrário de uma verificação de integridade do Route 53, um controle de roteamento não monitora os tempos de resposta ou os tempos de conexão TCP. Um controle de roteamento é um simples interruptor liga-desliga que controla uma verificação de integridade. Normalmente, você altera o estado para redirecionar o tráfego, e essa mudança de estado move o tráfego para um determinado endpoint para toda a pilha de aplicativos ou impede o roteamento para toda a pilha de aplicativos. Por exemplo, em um cenário simples, quando você altera um estado de controle de roteamento de On para `Off`, ele atualiza uma

verificação de integridade do Route 53, que você associou a um registro de failover de DNS para mover o tráfego de um endpoint.

Para atualizar um estado de controle de roteamento e redirecionar o tráfego, você deve se conectar a um dos seus endpoints de cluster no Route 53 ARC. Se o endpoint ao qual você está tentando se conectar não estiver disponível, tente alterar o estado com outro endpoint de cluster. Seu processo de alteração dos estados de controle de roteamento deve estar preparado para testar cada endpoint em rotação, pois os endpoints do cluster percorrem os estados disponíveis e indisponíveis para manutenção e atualizações regulares.

Ao criar controles de roteamento, você configura seus registros DNS para associar as verificações de integridade do controle de roteamento aos nomes DNS do Route 53 que estão na frente de cada réplica do aplicativo. Por exemplo, para controlar os failovers de tráfego em dois balanceadores de carga, um em cada uma das duas regiões, crie duas verificações de integridade do controle de roteamento e as associa a dois registros DNS, por exemplo, registros de alias com políticas de roteamento por failover, com os nomes de domínio dos respectivos balanceadores de carga.

Você também pode configurar cenários de failover de tráfego mais complexos usando o controle de roteamento do Route 53 ARC junto com as verificações de integridade e conjuntos de registros DNS do Route 53, usando registros DNS com políticas de roteamento ponderado. Para ver um exemplo detalhado, consulte a seção sobre failover de tráfego de usuários na seguinte postagem do blog da AWS: Criar aplicativos altamente resilientes usando o Controlador de recuperação de aplicações do Amazon Route 53, parte 2: pilha multirregional.

Um controle de roteamento no Route 53 ARC tem vários benefícios em relação ao redirecionamento do tráfego com verificações de integridade tradicionais. Por exemplo: .

- Um controle de roteamento oferece uma maneira de executar o failover de toda a pilha de aplicativos. Isso contrasta com o failover de componentes individuais de uma pilha, como fazem as instâncias do Amazon EC2, com base em verificações de integridade em nível de atributos.
- Um controle de roteamento oferece uma sobreposição manual simples e segura que você pode usar para deslocar o tráfego para fazer manutenção ou se recuperar de falhas quando os monitores internos não detectam um problema.
- Você pode usar um controle de roteamento junto com regras de segurança para evitar efeitos colaterais comuns que podem ocorrer com a automação totalmente automatizada baseada em verificação de integridade, como o failover para uma infraestrutura em espera que não está preparada para o failover.

# Criar componentes de controle de roteamento no Route 53 ARC

Esta seção explica como criar um cluster, controles de roteamento, verificações de integridade e painéis de controle para trabalhar com o controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53.

Comece criando um cluster para hospedar seus controles de roteamento e os painéis de controle que você usa para agrupá-los. Em seguida, crie controles de roteamento e verificações de integridade para que você possa redirecionar o tráfego para failover de uma célula para outra, de modo que o tráfego vá para sua réplica de backup, por exemplo.

Observe que você será cobrado por hora para cada cluster que crier. Normalmente, você só precisa de um cluster para hospedar os controles de roteamento e os painéis de controle para o gerenciamento do controle de recuperação de um aplicativo. Além disso, você pode configurar o compartilhamento de atributos usando o AWS Resource Access Manager, para que um cluster possa hospedar controles de roteamento e outros atributos do Route 53 ARC pertencentes a várias Contas da AWS. Para saber mais sobre o compartilhamento de recursos no Route 53 ARC, consulte Suporte entre contas para clusters no Route 53 ARC. Para obter informações sobre preços, consulte Preços do Controlador de recuperação de aplicativos do Amazon Route 53 e role para baixo até o Amazon Route 53.

Para usar controles de roteamento para fazer failover do tráfego, crie verificações de integridade do controle de roteamento e associe-as aos registros DNS do Amazon Route 53 para atributos em seu aplicativo. Como exemplo, digamos que você tenha duas células, uma que você configurou como a célula primária do seu aplicativo e a outra que você configurou como secundária, para a qual realizar o failover.

Para configurar verificações de integridade para o failover, faça o seguinte:

1. Crie um controle de roteamento para cada célula.
2. Crie uma verificação de integridade para cada controle de roteamento.
3. Crie dois registros DNS, por exemplo, dois registros de failover de DNS e associe uma verificação de integridade a cada um.

Outro cenário em que você pode criar um controle de roteamento é criar uma regra de segurança que seja uma regra de isolamento. Nesse caso, você não associa verificações de integridade e registros DNS ao controle de roteamento porque você o usará como um controle de roteamento de isolamento. Para ter mais informações, consulte Criação de regras de segurança no Route 53 ARC .

As etapas para criar os componentes para controle de roteamento no console do Route 53 ARC estão incluídas nessas seções. Para saber mais sobre como usar as operações da API de configuração de controle de recuperação com o Route 53 ARC, consulte o Operações de API de configuração do controle de recuperação.

Tópicos

- Criar um cluster no Route 53 ARC
- Criar um controle de roteamento no Route 53 ARC
- Criar uma verificação de integridade do controle de roteamento no Route 53 ARC
- Criar um painel de controle no Route 53 ARC

## Criar um cluster no Route 53 ARC

Você deve criar um cluster para hospedar controles de roteamento e painéis de controle no Route 53 ARC.

Um cluster é um conjunto de endpoints regionais redundantes nos quais você pode executar chamadas de API para atualizar ou obter o estado de um ou mais controles de roteamento. Um único cluster pode hospedar vários controles de roteamento.

> **Important**
>
> Lembre-se de que você será cobrado por hora por cada cluster que criar. Um cluster pode hospedar vários controles de roteamento e painéis para o gerenciamento do controle de recuperação, normalmente o suficiente para um aplicativo.

Para criar um cluster

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Clusters.
3. Insira um nome para o produto e, depois, escolha Criar.
4. Selecione Criar cluster.

# Criar um controle de roteamento no Route 53 ARC

Crie um controle de roteamento para cada célula para a qual você deseja encaminhar o tráfego. Por exemplo, quando você tem um aplicativo com atributos separados para fins de recuperação, você pode ter uma célula para cada Região da AWS e células aninhadas para cada zona de disponibilidade em cada região. Nesse cenário, você pode criar um controle de roteamento para cada célula e cada célula aninhada.

Ao criar controles de roteamento, lembre-se de que os nomes dos controles de roteamento devem ser exclusivos em cada painel de controle.

Depois de criar controles de roteamento para usar para redirecionar o tráfego, associe cada um a uma verificação de integridade. Isso permite rotear o tráfego para as células com base nos registros DNS que você associou a cada uma. Se você estiver configurando uma regra de isolamento como regra de segurança e criando um controle de roteamento de isolamento, não adicione uma verificação de integridade ao controle de roteamento.

Como criar um controle de roteamento

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Controle de roteamento.
3. Na página Controle de roteamento, escolha Criar e, em seguida, escolha um Controle de roteamento.
4. Insira um nome para seu controle de roteamento, escolha o cluster ao qual adicionar o controle e opte por adicioná-lo a um painel existente, inclusive usando o painel de controle padrão. Ou então, crie um novo painel de controle.
5. Se você optar por criar um novo painel de controle, escolha um cluster para criar o painel e, em seguida, insira um nome para ele.
6. Escolha Criar controle de roteamento.
7. Siga as etapas para nomear e criar o controle de roteamento.

# Criar uma verificação de integridade do controle de roteamento no Route 53 ARC

Associe uma verificação de integridade do controle de roteamento a cada controle que deseja usar para redirecionar o tráfego. Configure cada verificação de integridade com um registro DNS do Amazon Route 53, por exemplo, um registro DNS de failover. Em seguida, você pode redirecionar o tráfego no Controlador de recuperação de aplicações do Amazon Route 53 simplesmente atualizando o estado do controle de roteamento associado, para configurá-lo como `On` ou `Off`.

> **Note**
>
> Você não pode editar uma verificação de integridade do controle de roteamento existente para associá-la a um controle de roteamento diferente.

Como criar uma verificação de integridade do controle de roteamento

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Controle de roteamento.
3. Na página Controle de roteamento, escolha um controle de roteamento.
4. Na página de detalhes do Controle de roteamento, escolha Criar verificação de integridade.
5. Insira um nome para a verificação de integridade e escolha Criar.

Em seguida, crie registros DNS do Route 53 e associe suas verificações de integridade do controle de roteamento a cada um. Por exemplo, vamos supor que você queira usar dois registros de failover de DNS aos quais deseja associar as verificações de integridade do controle de roteamento. Para que o Route 53 ARC faça o failover correto do tráfego usando controles de roteamento, comece criando os dois registros de failover no Route 53: um primário e um secundário. Para obter mais informações sobre como configurar registros de failover de DNS, consulte Conceitos de verificação de integridade.

Ao criar o registro primário de failover, os valores devem ser semelhantes aos seguintes:

```
Name: myapp.yourdomain.com
```

```
Type: CNAME
Set Identifier: Primary
Failover: Primary
TTL: 0
Resource Records:
Value: cell1.yourdomain.com
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Os valores do registro secundário de failover devem ser semelhantes aos seguintes:

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Secondary
Failover: Secondary
TTL: 0
Resource Records:
Value: cell2.yourdomain.com
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Agora, digamos que você queira redirecionar o tráfego porque houve uma falha. Para fazer isso, atualize os estados de controle de roteamento associados para alterar o estado de controle de roteamento primário para `OFF` e o estado de controle de roteamento secundário para `ON`. Quando você faz isso, as verificações de integridade associadas impedem que o tráfego vá para a réplica primária e, em vez disso, o encaminham para a réplica secundária. Para obter mais informações sobre failover de tráfego com controles de roteamento, consulte Obter e atualizar estados de controle de roteamento usando a API do Route 53 ARC (recomendado).

Para conferir exemplos dos comandos da AWS CLI para criar controles de roteamento e as verificações de integridade associadas usando operações de API do Route 53 ARC, consulte Comece com o controle de roteamento usando a AWS CLI.

## Criar um painel de controle no Route 53 ARC

Um painel de controle no Controlador de recuperação de aplicações do Amazon Route 53 permite agrupar controles de roteamento relacionados. Um painel de controle pode ter controles de roteamento que representam um microsserviço dentro de um aplicativo, um aplicativo inteiro em si ou um grupo de aplicativos, dependendo do escopo do seu failover. Uma vantagem de agrupar os controles de roteamento em um painel de controle é que você pode usar regras de segurança com um painel de controle para ajudar a proteger as alterações no roteamento do tráfego.

Ao criar um cluster, o Route 53 ARC cria um painel de controle padrão. Você pode usar o painel de controle padrão para seus controles de roteamento ou criar um ou mais painéis para agrupar seus controles de roteamento. Observe que somente caracteres ASCII são suportados para nomes de painéis de controle.

As etapas para criar um painel de controle no console do Route 53 ARC estão incluídas nesta seção. Para obter informações sobre como usar as operações da API de configuração de controle de recuperação com o Route 53 ARC, consulte o Operações de API de configuração do controle de recuperação.

Como criar um painel de controle

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Controle de roteamento.
3. Na página Controle de roteamento, escolha Criar e, em seguida, escolha um Painel de controle.
4. Escolha um cluster para criar o painel de controle e, em seguida, insira um nome para ele.
5. Escolha Criar painel de controle.

# Visualizar e atualizar estados de controle de roteamento no Route 53 ARC

Esta seção descreve como visualizar e atualizar os estados de controle de roteamento no Controlador de recuperação de aplicações do Amazon Route 53. Os controles de roteamento são simples interruptores liga-desliga que gerenciam o fluxo de tráfego para as células do seu grupo de recuperação. Normalmente, as células são Regiões da AWS ou, às vezes, zonas de disponibilidade que incluem seus atributos. Quando um estado de controle de roteamento é On, o tráfego flui para a célula que é controlada por esse controle de roteamento.

Agrupe os controles de roteamento em painéis de controle, que são agrupamentos lógicos de failover. Ao abrir um painel de controle no console, por exemplo, você pode ver todos os controles de roteamento de um agrupamento de uma só vez, para ver onde o tráfego está fluindo.

Você pode atualizar um estado de controle de roteamento no console do Route 53 ARC ou usando a API do Route 53 ARC. Recomendamos atualizar os estados de controle de roteamento usando a API. Primeiro, o Route 53 ARC oferece extrema confiabilidade com a API no plano de dados para realizar essas ações. Isso é importante quando você está alterando esses estados, pois as

alterações do estado de roteamento falham entre as células ao redirecionar o tráfego do aplicativo. Além disso, usando a API, você pode tentar se conectar a diferentes endpoints de cluster em rotação, conforme necessário, se um endpoint de cluster ao qual você está tentando se conectar não estiver disponível.

Você pode atualizar um estado de controle de roteamento ou pode atualizar vários estados ao mesmo tempo. Por exemplo, talvez você queira definir um estado de controle de roteamento `Off` para impedir que o tráfego flua para uma célula, como uma zona de disponibilidade em que um aplicativo está experimentando maior latência. Ao mesmo tempo, talvez você queira definir outro estado de controle de roteamento 0n para iniciar o fluxo de tráfego para outra célula ou zona de disponibilidade. Nesse cenário, você pode atualizar os dois estados de controle de roteamento ao mesmo tempo, para que o tráfego continue fluindo.

Tópicos



## Obter e atualizar estados de controle de roteamento usando a API do Route 53 ARC (recomendado)

Recomendamos que você use operações de API do Controlador de Recuperação de Aplicações do Amazon Route 53 para obter ou atualizar estados de controle de roteamento usando um comando da AWS CLI ou código que você desenvolveu para usar as operações de API do Route 53 ARC com um dos AWS SDKs. Recomendamos usar operações de API, seja com a CLI ou em código, para trabalhar com estados de controle de roteamento em vez de usar o AWS Management Console.

O Route 53 ARC oferece extrema confiabilidade para o failover entre células (Regiões da AWS), atualizando os estados de controle de roteamento usando a API, pois eles são armazenados em um cluster altamente disponível. O Route 53 ARC garante que pelo menos três dos cinco endpoints regionais do cluster estejam sempre acessíveis para alterações no estado do controle de roteamento. Para obter ou alterar um estado de controle de roteamento usando a API, conecte-se a um dos endpoints do cluster regional. Se o endpoint não estiver disponível, tente conectar a outro endpoint do cluster.

Você pode ver a lista de endpoints de cluster regionais para seu cluster no console do Route 53 ou usando uma ação de API, DescribeCluster. O processo para obter e alterar os estados de controle

de roteamento deve testar cada endpoint em rotação, conforme necessário, pois os endpoints do cluster percorrem os estados disponíveis e indisponíveis para manutenção e atualizações regulares.

Fornecemos informações detalhadas e exemplos de código para usar as operações de API do Route 53 ARC a fim de obter e atualizar estados de controle de roteamento e trabalhar com endpoints de cluster regionais. Para obter mais informações, consulte:

- Para exemplos de código que explicam como alternar entre endpoints de cluster regionais para obter e definir estados de controle de roteamento, consulte Ações para o Application Recovery Controller usando AWS SDKs.
- Para obter informações sobre como usar a AWS CLI para obter e atualizar os estados de controle de roteamento, consulte Listar e atualizar os controles e estados de roteamento com a AWS CLI.

## Obter e atualizar estados de controle de roteamento no AWS Management Console

Você pode obter e atualizar os estados de controle de roteamento no AWS Management Console. No entanto, esteja ciente de que você não pode escolher endpoints de cluster regionais diferentes no console. Ou seja, não há um processo para escolher e alternar entre endpoints de cluster no console, como você pode fazer usando a API do Controlador de recuperação de aplicações do Amazon Route 53. Além disso, o console não está altamente disponível, enquanto o plano de dados do Route 53 ARC oferece extrema confiabilidade. Por esses motivos, recomendamos que você use a API do Route 53 ARC para obter e atualizar os estados de controle de roteamento para operações de produção.

Para obter mais recomendações sobre o uso do Route 53 ARC para failover, consulte Práticas recomendadas para o Controlador de recuperação de aplicações do Amazon Route 53.

Para visualizar e atualizar os controles de roteamento no console, siga as etapas nos procedimentos a seguir.

Como obter estados de controle de roteamento

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Controle de roteamento.
3. Na lista, escolha um painel de controle e visualize os controles de roteamento.

Como atualizar um ou vários estados de controle de roteamento

1. Abra o console do Amazon Route 53 em https://console.aws.amazon.com/route53/home.
2. Em Controlador de recuperação de aplicativos, escolha Controle de roteamento.
3. Escolha Ação e, em seguida, escolha Alterar roteamento de tráfego.
4. Atualize os estados de um ou mais controles de roteamento para serem `Off` ou `On`, dependendo de para onde você deseja que o tráfego flua ou pare de fluir para seu aplicativo.
5. Digite `confirm` na caixa de texto.
6. Escolha Atualizar roteamento de tráfego.

# Criação de regras de segurança no Route 53 ARC

Ao trabalhar com vários controles de roteamento ao mesmo tempo no Controlador de recuperação de aplicações do Amazon Route 53, você pode decidir que deseja implementar proteções para evitar consequências indesejadas. Por exemplo, talvez você queira evitar a desativação inadvertida de todos os controles de roteamento de uma aplicação, o que resultaria em um cenário de falha aberta. Ou talvez você queira implementar um interruptor principal liga-desliga para desativar um conjunto de controles de roteamento, talvez para evitar que a automação redirecione o tráfego. Para estabelecer proteções como essas para o controle de roteamento no Route 53 ARC, crie regras de segurança.

Configure as regras de segurança com uma combinação de controles de roteamento, regras e outras opções que você especifica. Cada regra de segurança está associada a um único painel de controle, mas um painel pode ter mais de uma regra de segurança. Ao criar regras de segurança, lembre-se de que os nomes delas devem ser exclusivos em cada painel de controle.

Tópicos



## Tipos de regras de segurança

Há dois tipos de regras de segurança que você pode usar para proteger o failover de maneiras diferentes, regras de afirmação e regras de isolamento.

### Regra de afirmação

Com uma regra de afirmação, quando você altera um ou um conjunto de estados de controle de roteamento, o Route 53 ARC impõe que os critérios definidos ao configurar a regra sejam atendidos, ou então os estados de controle de roteamento não são alterados.

Um exemplo de quando isso é útil é evitar um cenário de falha de abertura, como um cenário em que você impede o tráfego de ir para uma célula, mas não inicia o fluxo de tráfego para outra célula. Para evitar isso, uma regra de afirmação garante que pelo menos um controle de roteamento em um conjunto de controles em um painel esteja `On` em um determinado momento. Isso garante que o tráfego flua para pelo menos uma região ou zona de disponibilidade de um aplicativo.

Para ver um exemplo de comando da AWS CLI que cria uma regra de afirmação para impor esses critérios, consulte Criar regras de segurança em Comece com o controle de roteamento usando a AWS CLI.

Para obter informações detalhadas sobre as propriedades de operação da API da regra de afirmação, consulte AssertionRuleo Guia de referência da API Routing Control para o Amazon Route 53 Application Recovery Controller.

### Regra de isolamento

Com uma regra de isolamento, você pode impor uma chave liga-desliga geral sobre um conjunto de controles de roteamento para que a alteração desses estados seja aplicada com base em um conjunto de critérios que você especificar na regra. O critério mais simples é se um único controle de roteamento que você especificar como alternância estiver definido como `ON` ou `OFF`.

Para implementar isso, crie um controle de roteamento de isolamento de portas, para usar como alternância geral, e controles de roteamento de destino, para controlar o fluxo de tráfego para diferentes regiões ou zonas de disponibilidade. Em seguida, para evitar atualizações de estado manuais ou automatizadas nos controles de roteamento de destino que você configurou para a regra de isolamento, defina o estado do controle de roteamento de isolamento como `Off`. Para permitir atualizações, configure-o como `On`.

Para ver um exemplo de comando da AWS CLI que cria uma regra de controle que implementa esse tipo de opção geral, consulte Criar regras de segurança em Comece com o controle de roteamento usando a AWS CLI.

Para obter informações detalhadas sobre as propriedades de operação da API Gating Rule, consulte GatingRuleo Guia de referência da API Routing Control para o Amazon Route 53 Application Recovery Controller.

## Criar uma regra de segurança no console

As etapas desta seção explicam como criar uma regra de segurança no console do Route 53 ARC. As etapas são semelhantes, tanto para regras de afirmação quanto para regras de isolamento. As diferenças estão anotadas no procedimento.

Para saber mais sobre o uso de operações de API de controle de roteamento e recuperação com o Controlador de recuperação de aplicações do Amazon Route 53, consulte Operações de API de configuração do controle de recuperação.

Como criar uma regra de segurança

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Controle de roteamento.
3. Na página Controle de roteamento, escolha um painel de controle.
4. Na página de detalhes do painel de controle, escolha Ação e, em seguida, Adicionar regra de segurança.
5. Escolha um tipo de regra para adicionar: regra de afirmação ou regra de isolamento.
6. Escolha um nome e, opcionalmente, altere o período de espera.
7. Especifique as opções de configuração para a regra de segurança.

   - Para uma regra de afirmação, especifique os controles de roteamento que serão afirmados.
   - Para uma regra de isolamento, especifique o controle de roteamento de portão e os controles de roteamento de destino.

   Para ambas as regras, especifique a configuração da regra escolhendo o tipo, o limite e se a regra está invertida.

> **Note**
>
> Para saber mais sobre a especificação de uma regra de asserção, consulte as informações fornecidas para AssertionRuleoperação no Guia de referência da API Routing Control para o Amazon Route 53 Application Recovery Controller. Para saber mais sobre a especificação de uma regra de bloqueio, consulte as informações fornecidas para a GatingRuleoperação no Guia de referência da API Routing Control para o Amazon Route 53 Application Recovery Controller.

8. Selecione Create.

## Editar ou excluir uma regra de segurança no console

As etapas desta seção explicam como editar ou excluir uma regra de segurança no console do Route 53 ARC. Você só pode fazer edições limitadas em uma regra de segurança para alterar o nome ou atualizar o período de espera. Para fazer alterações mais abrangentes, exclua e recrie a regra de segurança.

Para saber mais sobre o uso de operações de API com o Controlador de recuperação de aplicações do Amazon Route 53, consulte o Operações de API comuns para o Controlador de Recuperação de Aplicações do Amazon Route 53.

Como excluir uma regra de segurança

1. Abra o console ARC do Route 53 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Controle de roteamento.
3. Na página Controle de roteamento, escolha um painel de controle.
4. Na página de detalhes do painel de controle, escolha uma regra de segurança e Excluir ou Editar.

## Sobrepor regras de segurança para redirecionar o tráfego

Há cenários em que você desejará sobrepor as proteções de controle de roteamento aplicadas com as regras de segurança que você configurou. Por exemplo, talvez você queira fazer o failover rapidamente para recuperação de desastres, e uma ou mais regras de segurança impeçam

inesperadamente que você atualize um estado de controle de roteamento para redirecionar o tráfego. Em um cenário de emergência como esse, você pode sobrepor uma ou mais regras de segurança para alterar o estado do controle de roteamento e fazer o failover do seu aplicativo.

Você pode sobrepor as regras de segurança ao atualizar um estado de controle de roteamento (ou vários) usando o comando `update-routing-control-state` ou o comando `update-routing-control-states` da AWS CLI com o parâmetro `safety-rules-to-override`. Especifique o parâmetro com o nome de recurso da Amazon (ARN) da regra de segurança que você deseja sobrepor ou especifique uma lista de ARNs, separada por vírgulas, para sobrepor duas ou mais regras de segurança.

Quando uma regra de segurança bloqueia uma atualização do estado do controle de roteamento, a mensagem de erro inclui o ARN da regra que bloqueou a atualização. Anote o ARN e, em seguida, especifique-o em um comando da CLI do estado de controle de roteamento com o parâmetro de sobreposição da regra de segurança.

> **Note**
>
> Como mais de uma regra de segurança pode estar em vigor para os controles de roteamento sendo atualizados, você pode executar o comando da CLI para atualizar o estado do controle de roteamento com uma sobreposição da regra de segurança, mas receber um erro informando que outra regra de segurança está bloqueando a atualização. Continue adicionando ARNs de regras de segurança à lista de regras a serem substituídas no comando de atualização, separados por vírgulas, até que o comando de atualização seja concluído com êxito.

Para saber mais sobre como usar a `SafetyRulesToOverride` propriedade com a API e os SDKs, consulte UpdateRoutingControlState.

A seguir estão dois exemplos de comandos da CLI para sobrepor as regras de segurança e atualizar os estados de controle de roteamento.

Sobrepor uma regra de segurança

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
```

```
    --routing-control-state On \
    --safety-rules-to-override arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888 \
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Sobrepor duas regras de segurança

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
    --routing-control-state On \
    --safety-rules-to-override "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888" \
    "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
qqqqqqq7777777"
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

# Suporte entre contas para clusters no Route 53 ARC

O Amazon Route 53 Application Recovery Controller se integra AWS Resource Access Manager para permitir o compartilhamento de recursos. AWS RAM é um serviço que permite compartilhar recursos com outras pessoas Contas da AWS ou por meio de AWS Organizations. Para o Route 53 ARC, você pode compartilhar o recurso de cluster.

Com AWS RAM, você compartilha recursos de sua propriedade criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os participantes com os quais compartilhá-los. Os participantes podem incluir:

- Específico Contas da AWS dentro ou fora da organização do proprietário em AWS Organizations
- 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.

Ao usar AWS Resource Access Manager para compartilhar recursos de cluster entre contas no Route 53 ARC, você pode usar um cluster para hospedar painéis de controle e controles de roteamento pertencentes a vários diferentes Contas da AWS. Quando você opta por compartilhar um cluster, outros Contas da AWS que você especificar podem usar o cluster para hospedar seus próprios painéis de controle e controles de roteamento, permitindo mais controle e flexibilidade sobre os recursos de roteamento em diferentes equipes.

AWS RAM é um serviço que ajuda AWS os clientes a compartilhar recursos com segurança entre eles. Contas da AWS Com AWS RAM, você pode compartilhar recursos dentro de uma organização ou unidades organizacionais (OUs) em AWS Organizations, usando funções e usuários do IAM. AWS RAM é uma forma centralizada e controlada de compartilhar um cluster.

Ao compartilhar um cluster, você pode reduzir o número total de clusters que sua organização exige. Com um cluster compartilhado, você pode alocar o custo total de execução do cluster em diferentes equipes, para maximizar os benefícios do Route 53 ARC com menor custo. (A criação de recursos hospedados em um cluster não tem custos adicionais, nem para o proprietário nem para os participantes.) O compartilhamento de clusters entre contas também pode facilitar o processo de integração de vários aplicativos ao Route 53 ARC, especialmente se você tiver um grande número de aplicativos distribuídos em várias contas e equipes de operações.

Para começar com o compartilhamento entre contas no Route 53 ARC, crie um compartilhamento de recursos no AWS RAM. O compartilhamento de recursos especifica os participantes autorizados a compartilhar o cluster que sua conta possui. Em seguida, os participantes podem criar recursos, como painéis de controle e controles de roteamento, no cluster, usando AWS Management Console ou executando as operações da API ARC do Route 53 usando os AWS SDKs AWS Command Line Interface ou.

Este tópico explica como compartilhar recursos que você possui e como usar os recursos que são compartilhados com você.

Conteúdo

- Cotas

## Pré-requisitos para compartilhar clusters

- Para compartilhar um cluster, você deve possuí-lo em seu Conta da AWS. Isso significa que o recurso deve ser alocado ou provisionado em sua conta. Não é possível compartilhar um cluster que tenha sido compartilhado com você.
- Para compartilhar um cluster com sua organização ou unidade organizacional no AWS Organizations, é preciso habilitar o compartilhamento no AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Manual do usuário do AWS RAM .

## Compartilhar um cluster

Quando você compartilha um cluster de sua propriedade, os participantes que você especifica para compartilhar o cluster podem criar e hospedar seus próprios recursos do Route 53 ARC no cluster.

Para compartilhar um cluster, é necessário 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 Contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os participantes com os quais compartilhá-los. Para compartilhar um cluster, crie um novo compartilhamento de recursos ou adicione o recurso a um compartilhamento de recursos existente. Para criar um novo compartilhamento de recursos, você pode usar o AWS RAM console ou usar operações de AWS RAM API com os AWS SDKs AWS Command Line Interface ou.

Se você faz parte de uma organização AWS Organizations e o compartilhamento dentro da sua organização está ativado, os participantes da sua organização recebem automaticamente acesso ao cluster compartilhado. Caso contrário, os participantes recebem um convite para participar do compartilhamento e obtêm acesso aos recursos do cluster após aceitarem o convite.

Você pode compartilhar um cluster de sua propriedade usando o AWS RAM console ou usando operações de AWS RAM API com os SDKs AWS CLI ou.

Para compartilhar um cluster que você possui usando o AWS RAM console

Consulte Creating a resource share no Guia do usuário do AWS RAM .

Para compartilhar um cluster que você possui usando o AWS CLI

Use o comando create-resource-share.

## Cancelar o compartilhamento de um cluster

Quando você cancela o compartilhamento de um cluster, o seguinte se aplica aos participantes e proprietários:

- Os recursos existentes dos participantes continuarão em existindo no cluster não compartilhado.
- Os participantes podem continuar atualizando os estados de controle de roteamento no cluster não compartilhado para gerenciar o roteamento para o failover dos aplicativos.
- Os participantes não poderão mais criar novos recursos no cluster não compartilhado.
- Se os participantes ainda tiverem recursos em um cluster não compartilhado, o proprietário não poderá excluir o cluster compartilhado.

Para cancelar o compartilhamento de um cluster de sua propriedade, é necessário removê-lo do compartilhamento de recursos. Você pode fazer isso usando o AWS RAM console ou usando operações de AWS RAM API com os SDKs AWS CLI ou.

Para cancelar o compartilhamento de um cluster compartilhado que você possui usando o console AWS RAM

Consulte Atualização de um compartilhamento de recursos no Manual do usuário do AWS RAM .

Para cancelar o compartilhamento de um cluster compartilhado que você possui usando o AWS CLI

Use o comando disassociate-resource-share.

## Identificar um cluster compartilhado

Proprietários e participantes podem identificar clusters compartilhados visualizando as informações no AWS RAM. Eles também podem obter informações sobre recursos compartilhados usando o console do Route 53 ARC e a AWS CLI.

Em geral, para saber mais sobre os recursos que você compartilhou ou que foram compartilhados com você, consulte as informações no Guia do AWS Resource Access Manager usuário:

- Como proprietário, você pode ver todos os recursos que está compartilhando com outras pessoas usando o AWS RAM. Para obter mais informações, consulte Visualizando seus recursos compartilhados em AWS RAM.

- Como participante, você pode visualizar todos os recursos compartilhados com você usando AWS RAM. Para obter mais informações, consulte Visualizando seus recursos compartilhados em AWS RAM.

Como proprietário, você pode determinar se está compartilhando um cluster visualizando as informações no AWS Management Console ou usando as operações da AWS Command Line Interface API ARC do Route 53.

Para identificar se um cluster seu está compartilhado usando o console

Na página AWS Management Console de detalhes de um cluster, consulte o status de compartilhamento do cluster.

Para identificar se um cluster que você possui é compartilhado usando o AWS CLI

Use o comando da get-resource-policy. Se houver uma política de recursos para um cluster, o comando retornará informações sobre ela.

Como participante, quando um cluster for compartilhado com você, normalmente você deverá aceitar o compartilhamento. Além disso, o campo Proprietário do cluster contém a conta do proprietário do cluster.

## Responsabilidades e permissões para clusters compartilhados

### Permissões para proprietários

Quando você compartilha um cluster que você possui com outras pessoas Contas da AWS, os participantes que têm permissão para usar o cluster podem criar painéis de controle, controles de roteamento e outros recursos no cluster.

Como proprietário do cluster, você é responsável por criar, gerenciar e excluir clusters. Você não pode modificar nem excluir recursos criados por participantes, como controles de roteamento e regras de segurança. Por exemplo, você não pode atualizar um controle de roteamento criado por um participante para alterar o estado do controle de roteamento.

No entanto, você pode visualizar os detalhes dos controles de roteamento criados pelos participantes em um cluster de sua propriedade. Por exemplo, você pode visualizar os estados de controle de roteamento chamando uma operação de API de controle de roteamento ARC do Route 53, usando os SDKs AWS Command Line Interface ou AWS .

Se você precisar modificar os recursos criados pelos participantes, eles podem configurar uma função no IAM com permissão para acessar os recursos e adicionar sua conta à função.

### Permissões para participantes

Em geral, os participantes podem criar e usar painéis de controle, controles de roteamento, regras de segurança e verificações de saúde que eles criam em um cluster compartilhado com eles. Eles só podem visualizar, modificar ou excluir recursos de clusters no cluster compartilhado se forem proprietários dos recursos. Por exemplo, os participantes podem criar e excluir regras de segurança para os painéis de controle que eles criaram.

As seguintes restrições se aplicam aos participantes:

- Os participantes não poderão visualizar, modificar ou excluir painéis de controle criados por outras contas usando um cluster compartilhado.
- Os participantes não podem visualizar, criar ou modificar controles de roteamento, incluindo estados de controle de roteamento, para recursos criados em um cluster compartilhado por outras contas.
- Os participantes não podem criar, modificar ou visualizar regras de segurança criadas por outras contas em um cluster compartilhado.
- Os participantes não podem adicionar recursos no painel de controle padrão em um cluster compartilhado porque ele pertence ao proprietário do cluster.

Conforme observado, os participantes não podem criar controles de roteamento no painel de controle padrão para um cluster compartilhado, porque o proprietário do cluster é dono do painel de controle padrão. No entanto, o proprietário do cluster pode criar um perfil do IAM entre contas que proporciona a permissão para acessar o painel de controle padrão do cluster. Em seguida, o proprietário pode conceder a um participante permissões para assumir a função, para que o participante possa acessar o painel de controle padrão e usá-lo da maneira que o proprietário especificou por meio das permissões da função.

## Custos de faturamento

O proprietário de um cluster no Route 53 ARC é cobrado pelos custos associados ao cluster. Não há custos adicionais, para proprietários de clusters ou participantes, para criar recursos hospedados em um cluster.

Para obter informações detalhadas sobre preços e exemplos, consulte os Preços do Controlador de recuperação de aplicações do Amazon Route 53 e role para baixo até o Controlador de recuperação de aplicações do Amazon Route 53.

## Cotas

Todos os recursos criados em um cluster compartilhado, incluindo recursos criados por todos os participantes com acesso ao cluster compartilhado, contam como cotas vigentes para o cluster e outros recursos, como controles de roteamento.

Para obter mais informações sobre cotas, consulte Cotas no Controlador de recuperação de aplicações do Amazon Route 53.

# Registrar e monitorar o Amazon Route 53 Application Recovery Controller

Você pode usar o Amazon CloudWatch e o AWS CloudTrail para monitorar o Controlador de Recuperação de Aplicações do Amazon Route 53, analisar padrões de tráfego e ajudar a solucionar problemas com recursos, como verificações de prontidão e clusters.

> **Note**
>
> Você deve visualizar as métricas e os registros do CloudWatch para o ARC do Route 53 na região Oeste dos EUA (Oregon), tanto no console quanto ao usar a AWS CLI. Ao usar a AWS CLI, especifique a região Oeste dos EUA (Oregon) para seu comando incluindo o seguinte parâmetro: `--region us-west-2`.

Tópicos



## Usando a Amazon CloudWatch com o Route 53 ARC

O Amazon Route 53 Application Recovery Controller publica pontos de dados na Amazon CloudWatch para suas verificações de prontidão. CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Por exemplo, você pode monitorar o tráfego em uma região da AWS durante um período de tempo especificado. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

Você pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um CloudWatch alarme para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica estiver fora do que você considera um intervalo aceitável.

Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

Tópicos



## Métricas do Route 53 ARC

O namespace `AWS/Route53RecoveryReadiness` inclui as métricas a seguir.

| Métrica | Descrição |
| --- | --- |
| `ReadinessChecks` | Representa o número de verificações de prontidão processadas pelo Route 53 ARC. A métrica pode ser dimensionada por seus estados, listados abaixo.<br><br>Unidade: `Count`.<br><br>Reporting criteria (Critérios de relatório): há um valor diferente de zero.<br><br>Estatísticas: a estatística mais útil é `Sum`.<br><br>Dimensões<br><br>• `READY`<br>• `NOT_READY`<br>• `NOT_AUTHORIZED`<br>• `UNKNOWN` |
| `Resources` | Representa o número de recursos processados pelo Route 53 ARC que podem ser dimensionados pelo identificador do recurso, conforme definido pela API.<br><br>Unidade: `Count`.<br><br>Reporting criteria (Critérios de relatório): há um valor diferente de zero. |

| Métrica | Descrição |
| --- | --- |
| | Estatísticas: a estatística mais útil é `Sum`.<br><br>Dimensões<br><br>• `ResourceSetType` : são os tipos de recursos, filtrados pelo número de recursos por determinado tipo avaliado pelo Route 53 ARC<br><br>Por exemplo: `AWS::CloudWatch::Alarm` |

## Estatísticas das métricas do Route 53 ARC

CloudWatch fornece estatísticas com base nos pontos de dados métricos publicados pelo Route 53 ARC. As estatísticas são agregações de dados de métrica ao longo de um período especificado. Quando você solicita estatísticas, o fluxo de dados apresentado é identificado pelo nome da métrica e pela dimensão. Dimensão é um par de nome/valor que identifica exclusivamente uma métrica.

Veja a seguir exemplos de combinações de métrica/dimensão que podem ser úteis:

- Veja o número de verificações de prontidão avaliadas pelo Route 53 ARC.
- Veja o número total de recursos para um determinado tipo de conjunto de recursos avaliado pelo Route 53 ARC.

## Exibir CloudWatch métricas no Route 53 ARC

Você pode visualizar as CloudWatch métricas do Route 53 ARC usando o CloudWatch console ou AWS CLI o. No console, essas métricas são exibidas como gráficos de monitoramento.

Você deve visualizar CloudWatch as métricas do Route 53 ARC na região Oeste dos EUA (Oregon), tanto no console quanto ao usar o. AWS CLI Ao usar a AWS CLI, especifique a região Oeste dos EUA (Oregon) para seu comando incluindo o seguinte parâmetro: `--region us-west-2`.

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. Selecione o namespace Route53 RecoveryReadiness.
4. (Opcional) Para visualizar uma métrica em todas as dimensões, digite o nome no campo de pesquisa.

Para visualizar métricas usando o AWS CLI

Use o comando list-metrics para listar as métricas disponíveis:

```
aws cloudwatch list-metrics --namespace AWS/Route53RecoveryReadiness --region us-west-2
```

Para obter as estatísticas de uma métrica usando a AWS CLI

Use o get-metric-statisticscomando a seguir para obter estatísticas para uma métrica e dimensão especificadas. Observe que CloudWatch trata cada combinação exclusiva de dimensões como uma métrica separada. Não é possível recuperar estatísticas usando combinações de dimensões que não tenham sido especificamente publicadas. Você deve especificar as mesmas dimensões usadas ao criar as métricas.

O exemplo a seguir lista o total de verificações de prontidão avaliadas, por minuto, para uma conta no Route 53 ARC.

```
aws cloudwatch get-metric-statistics --namespace AWS/Route53RecoveryReadiness \
--metric-name ReadinessChecks \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=State,Value=READY \
--start-time 2021-07-03T01:00:00Z --end-time 2021-07-03T01:20:00Z
```

A seguir está um exemplo de saída do comando:

```
{
    "Label": "ReadinessChecks",
    "Datapoints": [
        {
            "Timestamp": "2021-07-08T18:00:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
```

```
            "Timestamp": "2021-07-08T18:04:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:01:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:02:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:03:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        }
    ]
}
```

# Registrar chamadas da API do Route 53 ARC usando o AWS CloudTrail

O Amazon Route 53 Application Recovery Controller é integrado AWS CloudTrail a um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Route 53 ARC. CloudTrail captura todas as chamadas de API para o Route 53 ARC como eventos. As chamadas capturadas incluem as chamadas do console do Route 53 ARC e as chamadas de código para as operações de API dele.

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 ARC. 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 ao Route 53 ARC, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

# Informações do Route 53 ARC em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Route 53 ARC, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Para obter um registro de eventos em andamento na sua Conta da AWS, incluindo eventos do Route 53 ARC, 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 da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para 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 ARC do Route 53 são registradas CloudTrail e documentadas no Guia de referência da API Recovery Readiness para o Amazon Route 53 Application Recovery Controller, no Guia de referência da API de configuração de controle de recuperação do Amazon Route 53 Application Recovery Controller e no Guia de referência da API Routing Control para o Amazon Route 53 Application Recovery Controller. Por exemplo, chamadas para o `CreateCluster` `UpdateRoutingControlState` e `CreateRecoveryGroup` as ações 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 AWS Identity and Access Management
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.

- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

## Visualizar eventos do Route 53 ARC 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 ARC, você deve escolher Oeste dos EUA (Oregon) no seletor de região na parte superior do console. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário.

## Noções básicas sobre entradas de arquivos de log do Route 53 ARC

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 exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateCluster` ação para a configuração do controle.


```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:iam::111122223333:user/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/smithj",
              "accountId": "111122223333",
              "userName": "smithj"
          },
          "webIdFederationData": {},
          "attributes": {
```

```
                "mfaAuthenticated": "false",
                "creationDate": "2021-06-30T04:44:41Z"
            }
        }
    },
    "eventTime": "2021-06-30T04:45:46Z",
    "eventSource": "route53-recovery-control-config.amazonaws.com",
    "eventName": "CreateCluster",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
    "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
    "requestParameters": {
        "ClientToken": "12345abcdef-1234-5678-abcd-12345abcdef",
        "ClusterName": "XYZCluster"
    },
    "responseElements": {
        "Cluster": {
            "Arn": "arn:aws:route53-recovery-control::012345678901:cluster/abc123456-
aa11-bb22-cc33-abc123456",
            "ClusterArn": "arn:aws:route53-recovery-control::012345678901:cluster/
abc123456-aa11-bb22-cc33-abc123456",
            "Name": "XYZCluster",
            "Status": "PENDING"
        }
    },
    "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
    "eventID": "9cab44ef-0777-41e6-838f-f249example",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `UpdateRoutingControlState` ação do controle de roteamento.

```
{
    "eventVersion": "1.08",
     "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/admin/smithj",
```

```
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
           "sessionIssuer": {
               "type": "Role",
               "principalId": "A1B2C3D4E5F6G7EXAMPLE",
               "arn": "arn:aws:iam::111122223333:role/admin",
               "accountId": "111122223333",
               "userName": "admin"
           },
           "webIdFederationData": {},
           "attributes": {
               "mfaAuthenticated": "false",
               "creationDate": "2021-06-30T04:44:41Z"
           }
       }
  },
  "eventTime": "2021-06-30T04:45:46Z",
  "eventSource": "route53-recovery-control-config.amazonaws.com",
  "eventName": "UpdateRoutingControl",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.50",
  "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
  "requestParameters": {
      "RoutingControlName": "XYZRoutingControl3",
      "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
  },
  "responseElements": {
      "RoutingControl": {
          "ControlPanelArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
          "Name": "XYZRoutingControl3",
          "Status": "DEPLOYED",
          "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
      }
  },
  "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
  "eventID": "9cab44ef-0777-41e6-838f-f249example",
  "readOnly": false,
  "eventType": "AwsApiCall",
```

```
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateRecoveryGroup` ação para verificação de prontidão.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA33L3W36EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/admin",
                "accountId": "111122223333",
                "userName": "EXAMPLENAME"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-07-06T17:38:05Z"
            }
        }
    },
    "eventTime": "2021-07-06T18:08:03Z",
    "eventSource": "route53-recovery-readiness.amazonaws.com",
    "eventName": "CreateRecoveryGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
    "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
    "requestParameters": {
        "recoveryGroupName": "MyRecoveryGroup"
    },
    "responseElements": {
```

```
        "Access-Control-Expose-Headers": "x-amzn-errortype,x-amzn-requestid,x-amzn-
errormessage,x-amzn-trace-id,x-amzn-requestid,x-amz-apigw-id,date",
        "cells": [],
        "recoveryGroupName": "MyRecoveryGroup",
        "recoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/MyRecoveryGroup",
        "tags": "***"
    },
    "requestID": "fd42dcf7-6446-41e9-b408-d096example",
    "eventID": "4b5c42df-1174-46c8-be99-d67aexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `ListManagedResources` ação da mudança zonal.

```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
```

```
      "eventTime": "2022-11-14T16:14:41Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `StartZonalShift` ação com uma exceção de conflito para mudança zonal.

```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
```

```
        }
      },
      "eventTime": "2022-11-14T16:10:38Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "StartZonalShift",
     "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "errorCode": "ConflictException",
      "errorMessage": "There's already an active zonal shift for that resource
 identifier: 'arn:aws:testservice:us-west-2:077059137270:testResource/456apples'.
 Active zonal shift: 'bac23b74-176e-c073-de8f-484ca508910f'",
      "requestParameters": {
        "resourceIdentifier": "arn:aws:testservice:us-
west-2:077059137270:testResource/456apples",
        "awayFrom": "usw2-az1",
        "expiresIn": "2m",
        "comment": "HIDDEN_FOR_SECURITY_REASONS"
      },
      "responseElements": null,
      "requestID": "OP4OYXZ54HUPMIPGWH_EXAMPLE",
      "eventID": "0bca6660-e999-43a5-9008-EXAMPLE",
      "readOnly": false,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

# Usando o Route 53 ARC com a Amazon EventBridge

Usando a Amazon EventBridge, você pode configurar regras orientadas por eventos que monitoram seus recursos do Amazon Route 53 Application Recovery Controller e iniciam ações específicas que usam outros serviços. AWS Por exemplo, você pode definir uma regra para enviar notificações por e-mail sinalizando um tópico do Amazon SNS quando uma execução prática for iniciada para mudança automática de zona ou quando o status de uma verificação de prontidão mudar de PRONTO para NÃO PRONTO.

> **Note**
>
> O Route 53 ARC publica somente EventBridge eventos na região Oeste dos EUA (Oregon) (us-west-2). AWS Para receber EventBridge eventos para o Route 53 ARC, crie EventBridge regras na região Oeste dos EUA (Oregon).

Você pode criar regras na Amazon EventBridge para atuar em qualquer um dos seguintes eventos ARC do Route 53:

- Mudança de zona e mudança automática de zona. O evento especifica informações de status sobre mudanças de zona e mudanças automáticas para execução prática, por exemplo, quando uma execução prática está em andamento.
- Grupo de prontidão de recuperação. O evento especifica se o status de prontidão do grupo de recuperação muda, por exemplo, de PRONTO para NÃO PRONTO.
- Prontidão da célula. O evento especifica se o status de prontidão da célula muda, por exemplo, de PRONTO para NÃO PRONTO.
- Prontidão verifica prontidão. O evento especifica se o status da verificação de prontidão muda, por exemplo, de PRONTO para NÃO PRONTO.

Para capturar eventos ARC específicos do Route 53 nos quais você está interessado, defina padrões específicos de eventos que EventBridge possam ser usados para detectar os eventos. Os padrões de eventos têm a mesma estrutura que os eventos aos quais correspondem. O padrão menciona os campos com os quais você deseja fazer a correspondência e fornece os valores que você está procurando.

Os eventos são emitidos com base no melhor esforço. Eles são entregues do Route 53 ARC até quase EventBridge em tempo real em circunstâncias operacionais normais. No entanto, podem surgir situações que podem atrasar ou impedir a entrega de um evento.

Para obter informações sobre como EventBridge as regras funcionam com padrões de eventos, consulte Eventos e padrões de eventos em EventBridge.

## Monitore um recurso ARC do Route 53 com EventBridge

Com EventBridge, você pode criar regras que definem ações a serem tomadas quando o Route 53 ARC emite eventos para seus recursos. Por exemplo, você pode criar uma regra que envia uma

mensagem de e-mail quando o Route 53 ARC inicia uma execução prática para mudança automática de zona.

Para digitar ou copiar e colar um padrão de evento no EventBridge console, selecione a opção Inserir minha própria opção no console. Para ajudar a determinar padrões de eventos que podem ser úteis para você, este tópico inclui exemplos dos padrões de correspondência de eventos do Route 53 ARC e dos eventos do Route 53 ARC que você pode usar.

Para criar uma regra para um evento de recurso

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. Escolha Região da AWS aquela em que você deseja criar a regra. Para eventos de preparação, escolha Oeste dos EUA (Oregon). Para outros eventos, escolha a região na qual você tem interesse em assistir aos eventos.
3. Selecione Criar regra.
4. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.
5. Em Barramento de eventos, deixe o valor padrão, padrão.
6. Escolha Próximo.
7. Na etapa Criar padrão de eventos, em Origem do evento, deixe o valor padrão, Eventos da AWS.
8. Em Evento de amostra, escolha Inserir um próprio.
9. Em Eventos de amostra, digite ou copie e cole um padrão de eventos.

## Exemplo de padrões de eventos do Route 53 ARC

Os padrões de eventos têm a mesma estrutura que os eventos aos quais correspondem. O padrão menciona os campos com os quais você deseja fazer a correspondência e fornece os valores que você está procurando.

Você pode copiar e colar padrões de eventos desta seção EventBridge para criar regras que podem ser usadas para monitorar ações e recursos do ARC do Route 53.

### Exemplos de padrões de eventos de mudança automática de zona

Esta seção inclui exemplos de padrões de eventos que você pode usar EventBridge para o recurso de deslocamento automático zonal no Route 53 ARC.

Ao criar padrões de eventos para eventos de mudança automática de zona, você pode especificar qualquer um dos seguintes para `detail-type`:

- `Autoshift In Progress`
- `Autoshift Completed`
- `Practice Run Started`
- `Practice Run Succeeded`
- `Practice Run Interrupted`
- `Practice Run Failed`

Quando uma execução prática é interrompida, consulte o campo `additionalFailureInfo` para obter mais informações sobre o que causou a interrupção.

Para saber mais sobre a mudança automática de zona, incluindo execuções práticas, consulte Mudança automática de zona no Controlador de Recuperação de Aplicações do Amazon Route 53.

- Selecione todos os eventos da mudança automática de zona do Route 53 ARC.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ]
}
```

- Selecione todos os eventos da mudança automática de zona do Route 53 ARC em que uma execução prática foi iniciada.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Started"
    ]
}
```

- Selecione todos os eventos da mudança automática de zona do Route 53 ARC em que uma execução prática falhou.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Failed"
    ]
}
```

## Exemplos de padrões de eventos de verificação de prontidão

Os padrões de eventos a seguir fornecem exemplos que você pode usar EventBridge para o recurso de verificação de prontidão no Route 53 ARC.

- Selecione todos os eventos da verificação de prontidão do Route 53 ARC.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ]
}
```

- Selecione somente eventos relacionados às células.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ]
}
```

- Selecione somente eventos relacionados a uma célula específica chamada *`MyExampleCell`*.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
```

```
        "Route 53 Application Recovery Controller cell readiness status change"
    ],
    "resources": [
        "arn:aws:route53-recovery-readiness::111122223333:cell/MyExampleCell"
    ]
}
```

- Selecione somente eventos quando qualquer grupo de recuperação, célula ou status de verificação de prontidão se tornar *NOT READY*.

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail-type":{
      "new-state":{
         "readiness-status":[
            "NOT_READY"
         ]
      }
   }
}
```

- Selecione somente eventos quando qualquer grupo de recuperação, célula ou verificação de prontidão se tornar qualquer coisa, exceto *READY*

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail":{
      "new-state":{
         "readiness-status":[
            {
               "anything-but":"READY"
            }
         ]
      }
   }
}
```

# Exemplos de eventos do Route 53 ARC

Veja a seguir um exemplo de evento do Route 53 ARC para uma ação de mudança automática de zona:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Practice Run Interrupted",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": {
            "additionalFailureInfo": "Practice run interrupted. The blocking alarm
 entered ALARM state."
        },
        "metadata": {
            "awayFrom": "use1-az2"
        }
    }
}
```

Veja a seguir um exemplo de evento do Route 53 ARC para uma alteração no status de prontidão do grupo de recuperação:

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller recovery group readiness
 status change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:recovery-group/BillingApp"
```

```
    ],
    "detail": {
        "recovery-group-name": "BillingApp",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Veja a seguir um evento do Route 53 ARC para uma alteração de status de prontidão de uma célula:

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller cell readiness status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:cell/PDXCell"
    ],
    "detail": {
        "cell-name": "PDXCell",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Veja a seguir um evento do Route 53 ARC para uma alteração de status de verificação de prontidão:

```
{
    "version": "0",
    "account":"111122223333",
```

```
    "detail-type":"Route 53 Application Recovery Controller readiness check status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:readiness-check/
UserTableReadinessCheck"
    ],
    "detail": {
    "readiness-check-name": "UserTableReadinessCheck",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

## Especifique um grupo de CloudWatch registros para usar como destino

Ao criar uma EventBridge regra, você deve especificar o destino para o qual os eventos que correspondem à regra são enviados. Para obter uma lista dos alvos disponíveis para EventBridge, consulte Destinos disponíveis no EventBridge console. Um dos alvos que você pode adicionar a uma EventBridge regra é um grupo de CloudWatch registros da Amazon. Esta seção descreve os requisitos para adicionar grupos de CloudWatch registros como destinos e fornece um procedimento para adicionar um grupo de registros ao criar uma regra.

Para adicionar um grupo de CloudWatch registros como destino, você pode fazer o seguinte:

- Criar um novo grupo de registros
- Escolha um grupo de registros existente

Se você especificar um novo grupo de registros usando o console ao criar uma regra, EventBridge criará automaticamente o grupo de registros para você. Certifique-se de que o grupo de registros que você usa como destino para a EventBridge regra comece com `/aws/events`. Se você quiser escolher um grupo de registros existente, saiba que somente os grupos de registros que começam

com `/aws/events` aparecem como opções no menu suspenso. Para obter mais informações, consulte Criar um novo grupo de registros no Guia CloudWatch do usuário da Amazon.

Se você criar ou usar um grupo de CloudWatch registros para usar como destino usando CloudWatch operações fora do console, certifique-se de definir as permissões corretamente. Se você usar o console para adicionar um grupo de registros a uma EventBridge regra, a política baseada em recursos para o grupo de registros será atualizada automaticamente. Porém, se você usar o AWS Command Line Interface ou um AWS SDK para especificar um grupo de registros, deverá atualizar a política baseada em recursos para o grupo de registros. O exemplo de política a seguir ilustra as permissões que você deve definir em uma política baseada em recursos para o grupo de registros:

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

Você não pode configurar uma política baseada em recursos para um grupo de registros usando o console. Para adicionar as permissões necessárias a uma política baseada em recursos, use a operação da CloudWatch PutResourcePolicyAPI. Em seguida, você pode usar o comando describe-resource-policiesCLI para verificar se sua política foi aplicada corretamente.

Para criar uma regra para um evento de recurso e especificar um destino de grupo de CloudWatch registros

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.

2. Escolha Região da AWS aquela em que você deseja criar a regra.
3. Escolha Criar regra e, em seguida, insira qualquer informação sobre essa regra, como o padrão do evento ou os detalhes da programação.

   Para obter mais informações sobre a criação de EventBridge regras para o Route 53 ARC, consulte Monitorar um recurso ARC do Route 53 com EventBridge.
4. Na página Selecionar destino, escolha CloudWatchcomo seu alvo.
5. Escolha um grupo de CloudWatch registros no menu suspenso.

# Segurança no Controlador de recuperação de aplicações do Amazon Route 53

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Route 53 Application Recovery Controller, consulte AWS Services in Scope by Compliance Program AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da 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. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos ARC do Route 53.

Tópicos

# Proteção de dados no Controlador de recuperação de aplicações do Amazon Route 53

O modelo de responsabilidade AWS compartilhada O modelo se aplica à proteção de dados no Amazon Route 53 Application Recovery Controller. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou 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. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão 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 você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint 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 e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Route 53 ARC ou outro Serviços da AWS

usando o console, a API ou AWS os SDKs. AWS CLI 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.

### Criptografia em repouso

As informações de configuração do cliente são armazenadas em tabelas globais do Amazon DynamoDB, de propriedade do serviço, e são criptografadas em repouso.

Os conjuntos de dados que contêm o status das células em um cluster do Route 53 ARC são gravados em um volume do Amazon EBS para backup. O Route 53 ARC usa a criptografia padrão do Amazon EBS enquanto os dados estão em repouso.

### Criptografia em trânsito

As solicitações e respostas dos clientes para configuração do Route 53 ARC (consultas de status de prontidão, atualizações do estado da célula e assim por diante) são criptografadas durante o transporte em todo o serviço usando TLS.

## Gerenciamento de identidade e acesso no Controlador de recuperação de aplicações do Amazon Route 53

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado e autorizado para usar recursos do Route 53 ARC. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Conteúdo

- Exemplos de políticas baseadas em identidade do Controlador de recuperação de aplicações do Amazon Route 53
- Usar perfis vinculados ao serviço do Route 53 ARC
- AWS políticas gerenciadas para o Amazon Route 53 Application Recovery Controller
- Solução de problemas de identidade e acesso ao Controlador de recuperação de aplicação do Amazon Route 53

## Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Route 53 ARC.

Usuário do serviço: se você usar o serviço Route 53 ARC para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais recursos do Route 53 ARC para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Route 53 ARC, consulte Solução de problemas de identidade e acesso ao Controlador de recuperação de aplicação do Amazon Route 53.

Administrador do serviço: se você for o responsável pelos recursos do Route 53 ARC na empresa, provavelmente terá acesso total a ele. Cabe a você determinar quais funcionalidades e atributos do Route 53 ARC os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Route 53 ARC, consulte Como o Controlador de recuperação de aplicações do Amazon Route 53 funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Route 53 ARC. Para visualizar exemplos de políticas baseadas em identidade do Route 53 ARC que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade do Controlador de recuperação de aplicações do Amazon Route 53.

## Autenticando com identidades

A autenticação é 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 uma 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.

Independentemente 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 Guia do usuário do AWS IAM Identity Center e 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 Guia do usuário do AWS IAM Identity Center .

## Grupos e usuários 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 as 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 grupo chamado 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 uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) 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. Ela é semelhante a um usuário do IAM, mas não está associada 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 o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis 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 Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar 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 Guia do usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma 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 saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis 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 aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil 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.

- Perfil de serviço: um perfil de serviço é um perfil 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 Criar 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 a função 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 perfis vinculados ao 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 o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

## Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

### Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, grupo de usuários ou função do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

### Políticas baseadas em recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Como os SCPs funcionam no Guia do usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas

substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

### Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

## Como o Controlador de recuperação de aplicações do Amazon Route 53 funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Route 53 ARC, saiba quais recursos do IAM estão disponíveis para uso com ele.

Atributos do IAM que você pode usar com o Controlador de recuperação de aplicações do Amazon Route 53

| Recurso do IAM | Suporte do Route 53 ARC |
|---|---|
| Políticas baseadas em identidade | Sim |
| Políticas baseadas em recursos | Não |
| Ações de políticas | Sim |
| Recursos de políticas | Sim |
| Chaves de condição de políticas | Sim |
| ACLs | Não |
| ABAC (tags em políticas) | Parcial |
| Credenciais temporárias | Sim |
| Permissões de entidade principal | Sim |

| Recurso do IAM | Suporte do Route 53 ARC |
| --- | --- |
| Perfis de serviço | Não |
| Funções vinculadas ao serviço | Sim |

Para ter uma visão de alto nível de como o Route 53 ARC e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

## Políticas baseadas em identidade para o Route 53 ARC

| | |
| --- | --- |
| É compatível com políticas baseadas em identidade | Sim |

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. ‘Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Para visualizar exemplos de políticas baseadas em identidade do Route 53 ARC, consulte Exemplos de políticas baseadas em identidade do Controlador de recuperação de aplicações do Amazon Route 53.

## Políticas baseadas em recursos no Route 53 ARC

| | |
| --- | --- |
| Oferece suporte a políticas baseadas em recursos | Não |

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico.

## Ações das políticas para o Route 53 ARC

| | |
|---|---|
| Oferece suporte a ações de políticas | Sim |

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Route 53 ARC, consulte Ações definidas pelo Amazon Route 53 ARC na Referência de autorização do serviço.

As ações de políticas no Route 53 ARC usam os seguintes prefixos, dependendo da API com a qual você está trabalhando:

```
route53-recovery-readiness
route53-recovery-control-config
route53-recovery-cluster
arc-zonal-shift
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "route53-recovery-readiness:action1",
      "route53-recovery-readiness:action2"
         ]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

```
"Action": "route53-recovery-readiness:Describe*"
```

Para visualizar exemplos de políticas baseadas em identidade do Route 53 ARC, consulte Exemplos de políticas baseadas em identidade do Controlador de recuperação de aplicações do Amazon Route 53.

## Ações de políticas para o Route 53 ARC

| | |
|---|---|
| Oferece suporte a recursos de políticas | Sim |

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos e seus ARNs, e as ações que podem ser especificadas com o ARN de cada recurso, consulte os seguintes tópicos na Referência de autorização do serviço:

- Tipos de recursos definidos pelo cluster de recuperação no Amazon Route 53
- Tipos de recursos definidos pelos controles de recuperação no Amazon Route 53
- Tipos de recursos definidos pela prontidão de recuperação no Amazon Route 53
- Tipos de recursos definidos pela mudança de zona no Amazon Route 53

Para ver as ações e os recursos que você pode usar com uma chave de condição, consulte os tópicos a seguir na Referência de autorização de serviço:

- Ações definidas pelo cluster de recuperação do Amazon Route 53
- Ações definidas pelos controles de recuperação do Amazon Route 53
- Ações definidas pela prontidão de recuperação do Amazon Route 53
- Ações definidas pela mudança de zona do Amazon Route 53

Para visualizar exemplos de políticas baseadas em identidade do Route 53 ARC, consulte Exemplos de políticas baseadas em identidade do Controlador de recuperação de aplicações do Amazon Route 53.

## Chaves de condição de política para o Route 53 ARC

| | |
|---|---|
| Compatível com chaves de condição de política específicas do serviço | Sim |

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam atendentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de condição do Route 53 ARC, consulte Chaves de condição do Amazon Route 53 na Referência de autorização do serviço. Para saber com quais ações e recursos você pode usar a chave de condição, consulte Ações definidas pelo Controlador de recuperação de aplicações do Amazon Route 53.

Para ver uma lista das chaves de condição do Route 53 ARC, veja os tópicos a seguir na Referência de autorização do serviço:

- Chaves de condição para o cluster de recuperação do Amazon Route 53
- Chaves de condição para os controles de recuperação do Amazon Route 53
- Chaves de condição para a prontidão de recuperação do Amazon Route 53
- Chaves de condição da mudança de zona do Amazon Route 53

Para ver as ações e os recursos que você pode usar com uma chave de condição, consulte os tópicos a seguir na Referência de autorização de serviço:

- Ações definidas pelo cluster de recuperação do Amazon Route 53
- Ações definidas pelos controles de recuperação do Amazon Route 53
- Ações definidas pela prontidão de recuperação do Amazon Route 53
- Ações definidas pela mudança de zona do Amazon Route 53

Para visualizar exemplos de políticas baseadas em identidade do Route 53 ARC, consulte Exemplos de políticas baseadas em identidade do Controlador de recuperação de aplicações do Amazon Route 53.

## Listas de controle de acesso (ACLs) no Route 53 ARC

| | |
|---|---|
| Oferece suporte a ACLs | Não |

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

## Controle de acesso por atributo (ABAC) com o Route 53 ARC

| | |
|---|---|
| Oferece suporte a ABAC (tags em políticas) | Parcial |

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

O Route 53 ARC inclui o seguinte suporte parcial para ABAC:

- A verificação de prontidão e os controles de recuperação oferecem suporte ao ABAC.
- As mudanças de zona dão suporte ao ABAC para recursos gerenciados registrados no Route 53 ARC para mudança de zona. Para obter mais informações sobre o ABAC para o Network Load Balancer e os recursos gerenciados pelo Application Load Balancer, consulte ABAC com o Elastic Load Balancing no Guia do usuário do Elastic Load Balancing.
- O cluster de recuperação (controle de roteamento) não oferece suporte ao ABAC.

## Usar credenciais temporárias com o Route 53 ARC

| | |
|---|---|
| Oferece suporte a credenciais temporárias | Sim |

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS trabalhar com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para uma função (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

## Permissões de entidade principal entre serviços para o Route 53 ARC

| | |
|---|---|
| Suporte para o recurso Encaminhamento de sessões de acesso (FAS) | Sim |

Quando você usa uma entidade do IAM (usuário ou função) para realizar ações AWS, você é considerado principal. As políticas concedem permissões a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, aciona outra ação em outro serviço. Nesse caso, você precisa ter permissões para executar ambas as ações.

Para ver se uma ação requer ações dependentes adicionais em uma política, consulte a Referência de autorização do serviço.

- Cluster de recuperação do Amazon Route 53
- Controles de recuperação do Amazon Route 53
- Prontidão de recuperação do Amazon Route 53

- Mudança de zona do Amazon Route 53

### Perfis de serviço do Route 53 ARC

| | |
|---|---|
| Oferece suporte a perfis de serviço | Não |

A função de serviço é um perfil 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 Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

### Perfis vinculados ao serviço para o Route 53 ARC

| | |
|---|---|
| Oferece suporte a funções vinculadas ao serviço | Sim |

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir a função 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 perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados ao serviço do Route 53 ARC, consulte .

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte Serviços do AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço.

## IAM e permissões para mudança de zona

Esta seção descreve como as permissões funcionam para o recurso de mudança de zona fornecido pelo Amazon Route 53 Application Recovery Controller, especialmente se você trabalha com o recurso de outro AWS serviço, como o Elastic Load Balancing. Para saber como os atributos do

Route 53 ARC funcionam com o IAM e as permissões em geral, revise as informações em Como o Controlador de recuperação de aplicações do Amazon Route 53 funciona com o IAM.

Além das informações gerais de permissões que se aplicam ao Route 53 ARC, o seguinte se aplica à mudança de zona para IAM e permissões:

- Verifique se você tem as permissões necessárias para trabalhar com a mudança de zona no Route 53 ARC. Para obter mais informações, consulte Acesso ao console do Route 53 ARC e Acesso às ações do Route 53 ARC.
- Você não precisa agregar permissões adicionais do Elastic Load Balancing com o IAM para trabalhar com mudanças de zona para recursos gerenciados de balanceador de carga em sua conta no Route 53 ARC.
- Uma política AWS gerenciada que fornece acesso total ao Elastic Load Balancing inclui permissões para trabalhar com turnos zonais. Se você usa políticas AWS gerenciadas para acesso ao Elastic Load Balancing, não precisa de permissões adicionais no IAM para mudanças zonais para iniciar mudanças zonais para balanceadores de carga ou trabalhar com elas no console do Elastic Load Balancing. Para obter mais informações, consulte Políticas AWS gerenciadas pelo Elastic Load Balancing.

## Exemplos de políticas baseadas em identidade do Controlador de recuperação de aplicações do Amazon Route 53

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Route 53 ARC. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo Route 53 ARC, por exemplo, o formato dos ARNs para cada um dos tipos de recurso, consulte Ações, recursos e chaves de condição de identidade do Amazon Route 53 ARC na Referência de autorização do serviço.

Tópicos

- Práticas recomendadas de políticas
- Exemplo: acesso ao console do Route 53 ARC
- Exemplos: ações da API do Route 53 ARC

## Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Route 53 ARC em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e passe para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

## Exemplo: acesso ao console do Route 53 ARC

Para acessar o console do controlador de recuperação de aplicações do Amazon Route 53 ARC, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos ARC do Route 53 em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do Route 53 ARC quando você permite acesso somente a operações de API específicas, também anexe uma política `ReadOnly` AWS gerenciada para o Route 53 ARC às entidades. Para obter mais informações, consulte a página de políticas gerenciadas do Route 53 ARC ou Adicionar permissões a um usuário no Guia do usuário do IAM.

Para realizar algumas tarefas, os usuários devem ter permissão para criar um ou ambos os perfis de serviço associadas ao Route 53 ARC. Para saber mais sobre os perfis vinculados ao serviço do Route 53 ARC, consulte Usar perfis vinculados ao serviço do Route 53 ARC.

Para dar aos usuários acesso total ao uso dos atributos do Route 53 ARC por meio do console, anexe uma política como a seguinte para dar ao usuário permissões completas para configurar os recursos e operações do Route 53 ARC:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                  "route53-recovery-cluster:GetRoutingControlState",
                  "route53-recovery-cluster:UpdateRoutingControlState",
                  "route53-recovery-cluster:UpdateRoutingControlStates",
                  "route53-recovery-control-config:CreateCluster",
                  "route53-recovery-control-config:CreateControlPanel",
                  "route53-recovery-control-config:CreateRoutingControl",
                  "route53-recovery-control-config:CreateSafetyRule",
                  "route53-recovery-control-config:DeleteCluster",
                  "route53-recovery-control-config:DeleteControlPanel",
                  "route53-recovery-control-config:DeleteRoutingControl",
                  "route53-recovery-control-config:DeleteSafetyRule",
                  "route53-recovery-control-config:DescribeCluster",
                  "route53-recovery-control-config:DescribeControlPanel",
                  "route53-recovery-control-config:DescribeSafetyRule",
                  "route53-recovery-control-config:DescribeRoutingControl",
                  "route53-recovery-control-config:DescribeRoutingControlByName",
                  "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
                  "route53-recovery-control-config:ListClusters",
                  "route53-recovery-control-config:ListControlPanels",
                  "route53-recovery-control-config:ListRoutingControls",
                  "route53-recovery-control-config:ListSafetyRules",
                  "route53-recovery-control-config:UpdateControlPanel",
                  "route53-recovery-control-config:UpdateRoutingControl",
                  "route53-recovery-control-config:UpdateSafetyRule",
                  "route53-recovery-readiness:CreateCell",
                  "route53-recovery-readiness:CreateCrossAccountAuthorization",
                  "route53-recovery-readiness:CreateReadinessCheck",
                  "route53-recovery-readiness:CreateRecoveryGroup",
                  "route53-recovery-readiness:CreateResourceSet",
                  "route53-recovery-readiness:DeleteCell",
                  "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                  "route53-recovery-readiness:DeleteReadinessCheck",
                  "route53-recovery-readiness:DeleteRecoveryGroup",
                  "route53-recovery-readiness:DeleteResourceSet",
                  "route53-recovery-readiness:GetArchitectureRecommendations",
                  "route53-recovery-readiness:GetCell",
                  "route53-recovery-readiness:GetCellReadinessSummary",
                  "route53-recovery-readiness:GetReadinessCheck",
                  "route53-recovery-readiness:GetReadinessCheckResourceStatus",
                  "route53-recovery-readiness:GetReadinessCheckStatus",
                  "route53-recovery-readiness:GetRecoveryGroup",
                  "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                  "route53-recovery-readiness:GetResourceSet",
```

```
                "route53-recovery-readiness:ListCells",
                "route53-recovery-readiness:ListCrossAccountAuthorizations",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53-recovery-readiness:ListRecoveryGroups",
                "route53-recovery-readiness:ListResourceSets",
                "route53-recovery-readiness:ListRules",
                "route53-recovery-readiness:UpdateCell",
                "route53-recovery-readiness:UpdateReadinessCheck",
                "route53-recovery-readiness:UpdateRecoveryGroup",
                "route53-recovery-readiness:UpdateResourceSet",
                "arc-zonal-shift:ListManagedResources",
                "arc-zonal-shift:GetManagedResource",
                "arc-zonal-shift:ListZonalShifts",
                "arc-zonal-shift:StartZonalShift",
                "arc-zonal-shift:UpdateZonalShift",
                "arc-zonal-shift:CancelZonalShift",
                "arc-zonal-shift:CreatePracticeRunConfiguration",
                "arc-zonal-shift:DeletePracticeRunConfiguration",
                "arc-zonal-shift:ListAutoshifts",
                "arc-zonal-shift:UpdatePracticeRunConfiguration",
                "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                   "route53:GetHealthCheck",
                   "route53:CreateHealthCheck",
                   "route53:DeleteHealthCheck",
                   "route53:ChangeTagsForResource"
               ],
            "Resource": "*"
        }
        {
            "Effect": "Allow",
            "Action": [
                   "ec2:DescribeAvailabilityZones
               ],
            "Resource": "*"
        }
        {
            "Effect": "Allow",
            "Action": [
```

```
                "cloudwatch:DescribeAlarms
            ],
            "Resource": "*"
        }
    ]
}
```

## Exemplos: ações da API do Route 53 ARC

Há quatro APIs distintas que você pode usar com o Controlador de recuperação de aplicações do Amazon Route 53:

- A API de mudança zonal e mudança automática zonal, para funcionar com o plano de dados de mudança zonal ARC do Route 53 — para afastar temporariamente o tráfego de uma zona de disponibilidade para recuperar um aplicativo ou configurar o deslocamento automático zonal para que AWS afaste o tráfego de recursos do aplicativo de uma zona de disponibilidade, em seu nome, para ajudar a reduzir o tempo de recuperação durante eventos.
- A API de prontidão de recuperação, para trabalhar com o plano de controle de verificação de prontidão do Route 53 ARC e, por exemplo, criar grupos de recuperação, conjuntos de recursos e verificações de prontidão.
- A API de controle de recuperação, para trabalhar com o plano de controle de roteamento do Route 53 ARC, por exemplo, para criar clusters, painéis de controle e controles de roteamento.
- A API do plano de dados de controle de recuperação, para trabalhar com o plano de dados de controle de roteamento do Route 53 ARC, para consultar e atualizar os estados de controle de roteamento e realizar failover e recuperação regionais.

Para garantir que um usuário possa usar as ações de API do Route 53 ARC, anexe uma política que corresponda às operações de API com as quais o usuário precisa trabalhar, conforme descrito abaixo.

Para realizar algumas tarefas, os usuários devem ter permissão para criar um ou ambos os perfis de serviço associadas ao Route 53 ARC. Para saber mais sobre os perfis vinculados ao serviço do Route 53 ARC, consulte Usar perfis vinculados ao serviço do Route 53 ARC.

Para trabalhar com as operações de API de mudança automática de zona, anexe uma política como a seguinte ao usuário:

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arc-zonal-shift:CreatePracticeRunConfiguration",
                "arc-zonal-shift:DeletePracticeRunConfiguration",
                "arc-zonal-shift:ListAutoshifts",
                "arc-zonal-shift:UpdatePracticeRunConfiguration",
                "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
            "Resource": "*"
        }
        {
            "Effect": "Allow",
            "Action": [
                   "cloudwatch:DescribeAlarms
                ],
            "Resource": "*"
        }
    ]
}
```

Para trabalhar com as operações de API de mudança de zona, anexe uma política como a seguinte ao usuário:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        }
    ]
}
```

Para trabalhar com as operações de API de prontidão para recuperação, anexe uma política como a seguinte ao usuário:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-readiness:CreateCell",
                   "route53-recovery-readiness:CreateCrossAccountAuthorization",
                   "route53-recovery-readiness:CreateReadinessCheck",
                   "route53-recovery-readiness:CreateRecoveryGroup",
                   "route53-recovery-readiness:CreateResourceSet",
                   "route53-recovery-readiness:DeleteCell",
                   "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                   "route53-recovery-readiness:DeleteReadinessCheck",
                   "route53-recovery-readiness:DeleteRecoveryGroup",
                   "route53-recovery-readiness:DeleteResourceSet",
                   "route53-recovery-readiness:GetArchitectureRecommendations",
                   "route53-recovery-readiness:GetCell",
                   "route53-recovery-readiness:GetCellReadinessSummary",
                   "route53-recovery-readiness:GetReadinessCheck",
                   "route53-recovery-readiness:GetReadinessCheckResourceStatus",
                   "route53-recovery-readiness:GetReadinessCheckStatus",
                   "route53-recovery-readiness:GetRecoveryGroup",
                   "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                   "route53-recovery-readiness:GetResourceSet",
                   "route53-recovery-readiness:ListCells",
                   "route53-recovery-readiness:ListCrossAccountAuthorizations",
                   "route53-recovery-readiness:ListReadinessChecks",
                   "route53-recovery-readiness:ListRecoveryGroups",
                   "route53-recovery-readiness:ListResourceSets",
                   "route53-recovery-readiness:ListRules",
                   "route53-recovery-readiness:ListTagsForResources",
                   "route53-recovery-readiness:UpdateCell",
                   "route53-recovery-readiness:UpdateReadinessCheck",
                   "route53-recovery-readiness:UpdateRecoveryGroup",
                   "route53-recovery-readiness:UpdateResourceSet",
                   "route53-recovery-readiness:TagResource",
                   "route53-recovery-readiness:UntagResource"
             ],
            "Resource": "*"
```

```
        }
    ]
}
```

Para trabalhar com as operações de API de controle de recuperação, anexe uma política como a seguinte ao usuário:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-control-config:CreateCluster",
                   "route53-recovery-control-config:CreateControlPanel",
                   "route53-recovery-control-config:CreateRoutingControl",
                   "route53-recovery-control-config:CreateSafetyRule",
                   "route53-recovery-control-config:DeleteCluster",
                   "route53-recovery-control-config:DeleteControlPanel",
                   "route53-recovery-control-config:DeleteRoutingControl",
                   "route53-recovery-control-config:DeleteSafetyRule",
                   "route53-recovery-control-config:DescribeCluster",
                   "route53-recovery-control-config:DescribeControlPanel",
                   "route53-recovery-control-config:DescribeSafetyRule",
                   "route53-recovery-control-config:DescribeRoutingControl",
                   "route53-recovery-control-config:DescribeRoutingControlByName",
                   "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
                   "route53-recovery-control-config:ListClusters",
                   "route53-recovery-control-config:ListControlPanels",
                   "route53-recovery-control-config:ListRoutingControls",
                   "route53-recovery-control-config:ListSafetyRules",
                   "route53-recovery-control-config:ListTagsForResource",
                   "route53-recovery-control-config:UpdateControlPanel",
                   "route53-recovery-control-config:UpdateRoutingControl",
                   "route53-recovery-control-config:UpdateSafetyRule",
                   "route53-recovery-control-config:TagResource",
                   "route53-recovery-control-config:UntagResource"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "route53:GetHealthCheck",
                "route53:CreateHealthCheck",
                "route53:DeleteHealthCheck",
                "route53:ChangeTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Para realizar tarefas no Route 53 ARC com a API do plano de dados do cluster de recuperação, por exemplo, atualizando estados de controle de roteamento para failover durante um evento de desastre, você pode anexar uma política do IAM do Route 53 ARC como a seguinte ao seu usuário do IAM.

O `AllowSafetyRuleOverride` booleano dá permissão para substituir as regras de segurança que você configurou como proteção para controles de roteamento. Essa permissão pode ser necessária em cenários de emergência para contornar as proteções em desastres ou outros cenários urgentes de failover. Por exemplo, um operador pode precisar fazer o failover rapidamente para a recuperação de desastres, e uma ou mais regras de segurança podem impedir inesperadamente a atualização do estado do controle de roteamento necessária para redirecionar o tráfego. Essa permissão permite que o operador especifique regras de segurança a serem substituídas ao fazer chamadas de API para atualizar os estados de controle de roteamento. Para ter mais informações, consulte Sobrepor regras de segurança para redirecionar o tráfego.

Se você quiser permitir que um operador use a API do plano de dados do cluster de recuperação, mas evitar sobrepor as regras de segurança, você pode anexar uma política como a seguinte, mas definir o `AllowSafetyRuleOverrides` booleano como `false`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-cluster:GetRoutingControlState",
                "route53-recovery-cluster:ListRoutingControls"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlStates",
                "route53-recovery-cluster:UpdateRoutingControlState"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "route53-recovery-cluster:AllowSafetyRulesOverrides": "true"
                }
            }
        }
    ]
}
```

## Usar perfis vinculados ao serviço do Route 53 ARC

O Amazon Route 53 Application Recovery Controller usa AWS Identity and Access Management funções vinculadas a serviços (IAM). Um perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM que é vinculado diretamente a um serviço (nesse caso, o Route 53 ARC). As funções vinculadas ao serviço são predefinidas pelo Route 53 ARC e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome para fins específicos.

Perfis vinculados ao serviço facilitam a configuração do Route 53 ARC porque você não precisa adicionar as permissões necessárias manualmente. O Route 53 ARC define as permissões de seus perfis vinculados ao serviço e, exceto se definido de outra forma, somente o Route 53 ARC pode assumir seus perfis. As permissões definidas incluem as políticas de confiança e de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus recursos do Route 53 ARC, pois não é possível remover as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados a serviços, consulte Serviços da AWS compatíveis com o IAM e procure serviços que tenham Sim na coluna de Perfil vinculado ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

O Route 53 ARC tem os seguintes perfis vinculados ao serviço, que estão descritos neste capítulo:

- O Route 53 ARC usa a função vinculada ao serviço chamada Route53 RecoveryReadinessServiceRolePolicy para acessar recursos e configurações para verificar a prontidão.
- O Route 53 ARC usa a função vinculada ao serviço nomeada AWSServiceRoleForZonalAutoshiftPracticeRunpara execuções práticas de mudança automática, para monitorar CloudWatch alarmes e AWS Health Dashboard eventos de clientes da Amazon fornecidos pelo cliente e para iniciar execuções práticas.

## Permissões de função vinculadas ao serviço para o Route53 RecoveryReadinessServiceRolePolicy

O Route 53 ARC usa uma função vinculada ao serviço chamada Route53 RecoveryReadinessServiceRolePolicy para acessar recursos e configurações para verificar a prontidão. Esta seção descreve as permissões para o perfil vinculado ao serviço e as informações sobre como criar, editar e excluir o perfil.

Permissões de função vinculadas ao serviço para o Route53 RecoveryReadinessServiceRolePolicy

Esse perfil vinculado ao serviço usa a política gerenciada `Route53RecoveryReadinessServiceRolePolicy`.

A função RecoveryReadinessServiceRolePolicy vinculada ao serviço Route53 confia no seguinte serviço para assumir a função:

- `route53-recovery-readiness.amazonaws.com`

Para ver as permissões dessa política, consulte Route53 RecoveryReadinessServiceRolePolicy na Referência de política AWS gerenciada.

Criando a função RecoveryReadinessServiceRolePolicy vinculada ao serviço Route53 para o Route 53 ARC

Você não precisa criar manualmente a função vinculada ao RecoveryReadinessServiceRolePolicy serviço Route53. Quando você cria a primeira verificação de prontidão ou autorização entre contas na AWS Management Console, na ou na AWS API AWS CLI, o Route 53 ARC cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria a primeira verificação de

prontidão ou autorização entre contas, o Route 53 ARC cria o perfil vinculado ao serviço para você novamente.

Editando a função RecoveryReadinessServiceRolePolicy vinculada ao serviço Route53 para o Route 53 ARC

O Route 53 ARC não permite que você edite a função vinculada ao RecoveryReadinessServiceRolePolicy serviço Route53. Depois de criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois outras entidades podem fazer referência a ele. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo a função vinculada ao RecoveryReadinessServiceRolePolicy serviço Route53 para o Route 53 ARC

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. 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.

Depois de remover suas verificações de prontidão e suas autorizações entre contas, você pode excluir a função vinculada ao serviço RecoveryReadinessServiceRolePolicyRoute53. Para obter mais informações sobre verificações de prontidão, consulte Verificação de prontidão do Controlador de recuperação de aplicações do Amazon Route 53. Para obter informações sobre autorizações entre contas, consulte Criar autorizações entre contas no Route 53 ARC.

> **Note**
>
> Se o serviço Route 53 ARC estiver usando o perfil quando você tentar excluir os recursos, a exclusão do perfil de serviço poderá falhar. Se isso acontecer, espere alguns minutos e tente excluir o perfil novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função vinculada ao RecoveryReadinessServiceRolePolicy serviço Route53. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

## Permissões de função vinculadas ao serviço para AWSServiceRoleForZonalAutoshiftPracticeRun

O Route 53 ARC usa a função vinculada ao serviço chamada AWSServiceRoleForZonalAutoshiftPracticeRunpara fazer o seguinte:

- Monitore os CloudWatch alarmes e AWS Health Dashboard eventos de clientes da Amazon fornecidos pelo cliente para ensaios
- Gerenciar execuções práticas (mudanças de zona práticas)

Esta seção descreve as permissões para o perfil vinculado ao serviço e as informações sobre como criar, editar e excluir o perfil.

Permissões de função vinculadas ao serviço para AWSServiceRoleForZonalAutoshiftPracticeRun

Essa função vinculada ao serviço usa a política gerenciada. AWSZonalAutoshiftPracticeRunSLRPolicy

A função vinculada ao serviço AWSServiceRoleForZonalAutoshiftPracticeRun confia no seguinte serviço para assumir a função:

- `practice-run.arc-zonal-shift.amazonaws.com`

A política de permissões da função permite que o Route 53 ARC conclua as seguintes ações nos recursos especificados:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "MonitoringPermissions",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:DescribeAlarms",
    "health:DescribeEvents"
   ],
   "Resource": "*"
  },
  {
   "Sid": "ZonalShiftManagementPermissions",
```

```
    "Effect": "Allow",
    "Action": [
     "arc-zonal-shift:CancelZonalShift",
     "arc-zonal-shift:GetManagedResource",
     "arc-zonal-shift:StartZonalShift",
     "arc-zonal-shift:UpdateZonalShift"
    ],
    "Resource": "*"
   }
  ]
}
```

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado ao serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM.

Criando a função AWSServiceRoleForZonalAutoshiftPracticeRunvinculada ao serviço para o Route 53 ARC

Você não precisa criar manualmente a função vinculada a serviço AWSServiceRoleForZonalAutoshiftPracticeRun. Quando você cria a primeira configuração de execução prática no AWS Management Console, no ou em um AWS SDK AWS CLI, o Route 53 ARC cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria a primeira configuração de execução prática, o Route 53 ARC cria um perfil vinculado ao serviço para você novamente.

Editando a função AWSServiceRoleForZonalAutoshiftPracticeRunvinculada ao serviço para o Route 53 ARC

O Route 53 ARC não permite que você edite a função AWSServiceRoleForZonalAutoshiftPracticeRunvinculada ao serviço. Depois de criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois outras entidades podem fazer referência a ele. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo a função AWSServiceRoleForZonalAutoshiftPracticeRunvinculada ao serviço do Route 53 ARC

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja

monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de um perfil vinculado ao serviço antes de excluí-lo manualmente.

Depois de desativar o deslocamento automático, você poderá excluir a função vinculada ao AWSServiceRoleForZonalAutoshiftPracticeRunserviço. Para obter mais informações sobre o recurso de mudança automática, consulte Mudança de zona no Controlador de recuperação de aplicações do Amazon Route 53.

> **Note**
>
> Se o serviço Route 53 ARC estiver usando o perfil quando você tentar excluir os recursos, a exclusão do perfil de serviço poderá falhar. Se isso acontecer, espere alguns minutos e tente excluir o perfil novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForZonalAutoshiftPracticeRun vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

### Atualizações para o perfil vinculado ao serviço do Route 53 ARC

Para atualizações das políticas AWS gerenciadas para as funções vinculadas ao serviço do Route 53 ARC, consulte a tabela de atualizações de políticas AWS gerenciadas. Você também pode assinar alertas automáticos de RSS na Página de histórico de documentos do Route 53 ARC.

## AWS políticas gerenciadas para o Amazon Route 53 Application Recovery Controller

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 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 obter mais informações, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM.

## AWS política gerenciada: Route53 RecoveryReadinessServiceRolePolicy

Não é possível anexar `Route53RecoveryReadinessServiceRolePolicy` às entidades do IAM. Esta política é anexada a um perfil vinculado ao serviço que permite que o Amazon Route 53 acesse os serviços da AWS e recursos que são usados ou gerenciados pelo Route 53 ARC. Para ter mais informações, consulte Usar perfis vinculados ao serviço do Route 53 ARC.

## AWS política gerenciada: AmazonRoute 53 RecoveryReadinessFullAccess

Você pode anexar `AmazonRoute53RecoveryReadinessFullAccess` às entidades do IAM. Essa política concede acesso total às ações para trabalhar com prontidão de recuperação (verificação de prontidão) no Route 53 ARC. Anexe-a aos usuários do IAM e a outras entidades principais que precisam de acesso completo a ações de prontidão de recuperação.

Para ver as permissões dessa política, consulte AmazonRoute53 RecoveryReadinessFullAccess na Referência de política AWS gerenciada.

## AWS política gerenciada: AmazonRoute 53 RecoveryReadinessReadOnlyAccess

Você pode anexar `AmazonRoute53RecoveryReadinessReadOnlyAccess` às entidades do IAM. Esta política concede acesso somente leitura a ações para trabalhar com prontidão para recuperação no Route 53 ARC. É útil para usuários que precisam visualizar os status de prontidão e as configurações do grupo de recuperação. Esses usuários não podem criar, atualizar ou excluir recursos de prontidão de recuperação.

Para ver as permissões dessa política, consulte AmazonRoute53 RecoveryReadinessReadOnlyAccess na Referência de política AWS gerenciada.

## AWS política gerenciada: AmazonRoute 53 RecoveryControlConfigFullAccess

Você pode anexar `AmazonRoute53RecoveryControlConfigFullAccess` às entidades do IAM. Essa política concede acesso total às ações para trabalhar com a configuração de controle de

recuperação no Route 53 ARC. Anexe-a aos usuários do IAM e a outras entidades principais que precisam de acesso completo às ações de configuração de controle de recuperação.

Você pode agregar um acesso a ações adicionais do Amazon Route 53 para que os usuários criem verificações de integridade para controles de roteamento. Por exemplo, você pode dar permissão para uma ou mais das seguintes ações: `route53:GetHealthCheck`, `route53:CreateHealthCheck`, `route53:DeleteHealthCheck`, e `route53:ChangeTagsForResource`.

Para ver as permissões dessa política, consulte AmazonRoute53 RecoveryControlConfigFullAccess na Referência de política AWS gerenciada.

## AWS política gerenciada: AmazonRoute 53 RecoveryControlConfigReadOnlyAccess

Você pode anexar `AmazonRoute53RecoveryControlConfigReadOnlyAccess` às entidades do IAM. É útil para usuários que precisam visualizar as configurações de controles de roteamento e de regras de segurança. Esta política concede acesso somente leitura a ações para trabalhar com a configuração de controle de recuperação no Route 53 ARC. Esses usuários não podem criar, atualizar nem excluir recursos de controle de recuperação.

Para ver as permissões dessa política, consulte AmazonRoute53 RecoveryControlConfigReadOnlyAccess na Referência de política AWS gerenciada.

## AWS política gerenciada: AmazonRoute 53 RecoveryClusterFullAccess

Você pode anexar `AmazonRoute53RecoveryClusterFullAccess` às entidades do IAM. Essa política concede acesso total às ações para trabalhar com o plano de dados do cluster no Route 53 ARC. Anexe-a aos usuários do IAM e a outras entidades principais que precisam de acesso completo para atualizar e recuperar estados de controle de roteamento.

Para ver as permissões dessa política, consulte AmazonRoute53 RecoveryClusterFullAccess na Referência de política AWS gerenciada.

## AWS política gerenciada: AmazonRoute 53 RecoveryClusterReadOnlyAccess

Você pode anexar `AmazonRoute53RecoveryClusterReadOnlyAccess` às entidades do IAM. Esta política concede acesso somente leitura ao plano de dados do cluster no Route 53 ARC. Esses usuários podem recuperar estados de controle de roteamento, mas não podem atualizá-los.

Para ver as permissões dessa política, consulte AmazonRoute53 RecoveryClusterReadOnlyAccess na Referência de política AWS gerenciada.

## Atualizações do Route 53 ARC para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Route 53 ARC desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, assine o feed RSS na página Histórico de documentos do Route 53 ARC.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSServiceRoleForPercPracticePolicy— Nova política | O Route 53 ARC adicionou um novo perfil vinculado ao serviço para mudança automática e execuções práticas.<br><br>O Route 53 ARC usa as permissões habilitadas pela função vinculada ao serviço para monitorar alarmes e eventos de clientes CloudWatch da Amazon fornecidos pelo AWS Health Dashboard cliente para ensaios e para iniciar os treinos.<br><br>Para saber mais sobre o novo perfil vinculado ao serviço, consulte Permissões de função vinculadas ao serviço para AWSServiceRoleForZonalAutoshiftPracticeRun. | 30 de novembro de 2023 |
| AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Política atualizada | Adiciona permissões para`GetResourcePolicy` , para apoiar o retorno de detalhes sobre políticas AWS Resource Access Manager | 18 de outubro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | de recursos para recursos compartilhados. | |
| Route53 RecoveryReadinessServiceRolePolicy — Política atualizada | O Route 53 ARC adicionou novas permissões para consultar informações sobre instâncias do Amazon EC2.<br><br>O Route 53 ARC usa as seguintes permissões para apoiar a pesquisa de instâncias do Amazon EC2, executar verificações de prontidão e determinar o status de prontidão das instâncias.<br><br>`ec2:DescribeVpnGateways`<br><br>`ec2:DescribeCustomerGateways` | 17 de fevereiro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Route53 RecoveryReadinessServiceRolePolicy — Política atualizada | O Route 53 ARC adicionou uma nova permissão para consultar informações sobre funções do Lambda.<br><br>O Route 53 ARC usa a seguinte permissão para consultar informações sobre as funções do Lambda para executar verificações de prontidão e determinar o status de prontidão das funções.<br><br>`lambda:ListProvisionedConcurrencyConfigs` | 31 de agosto de 2022 |
| AmazonRoute53 RecoveryControlConfigFullAccess — Política atualizada | As permissões da política do Amazon Route 53 foram removidas e uma nota listando as permissões opcionais foi adicionada. | 26 de maio de 2022 |
| AmazonRoute53 RecoveryControlConfigFullAccess — Política atualizada | Foram adicionadas as permissões necessárias do Amazon Route 53 que faltavam à política. | 15 de abril de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRoute53 RecoveryClusterReadOnlyAccess — Política atualizada | O Route 53 ARC adicionou uma nova permissão, `route53-recovery-cluster:ListRoutingControls` , para permitir listar ARNs de controle de roteamento com alta disponibilidade. | 15 de março de 2022 |
| AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Política atualizada | O Route 53 ARC adicionou uma nova permissão, `route53-recovery-control-config:ListTagsForResources` , para permitir a listagem de tags para um recurso. | 20 de dezembro de 2021 |
| Route53 RecoveryReadinessServiceRolePolicy — Política atualizada | O Route 53 ARC adicionou uma nova permissão para consultar informações sobre o Amazon API Gateway.<br><br>O Route 53 ARC usa a permissão, `apigateway:GET` , para consultar informações sobre o API Gateway para executar verificações de prontidão e determinar o status de prontidão. | 28 de outubro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonRoute53 RecoveryReadinessReadOnlyAccess — Novas permissões adicionadas | O Route 53 ARC adicionou duas novas permissões ao AmazonRoute53 RecoveryReadinessReadOnlyAccess:<br><br>O Route 53 ARC usa `route53-recovery-readiness:GetArchitectureRecommendations` e `route53-recovery-readiness:GetCellReadinessSummary` para permitir acesso somente de leitura a essas ações e trabalhar com a prontidão de recuperação. | 15 de outubro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Route53 RecoveryReadinessServiceRolePolicy — Política atualizada | O Route 53 ARC adicionou novas permissões para consultar informações sobre as funções do Lambda.<br><br>O Route 53 ARC usa as seguintes permissões para consultar informações sobre as funções do Lambda para executar verificações de prontidão e determinar o status de prontidão dessas funções.<br><br>`lambda:GetFunctionConcurrency`<br><br>`lambda:GetFunctionConfiguration`<br><br>`lambda:GetProvisionedConcurrencyConfig`<br><br>`lambda:ListAliases`<br><br>`lambda:ListVersionsByFunction`<br><br>`lambda:ListEventSourceMappings`<br><br>`lambda:ListFunctions` | 8 de outubro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Route53 RecoveryReadinessServiceRolePolicy — Novas políticas gerenciadas adicionadas | O Route 53 ARC adicionou as seguintes novas políticas gerenciadas:<br><br>AmazonRoute53 RecoveryReadinessFullAccess<br><br>AmazonRoute53 RecoveryReadinessReadOnlyAccess<br><br>AmazonRoute53 RecoveryClusterFullAccess<br><br>AmazonRoute53 RecoveryClusterReadOnlyAccess<br><br>AmazonRoute53 RecoveryControlConfigFullAccess<br><br>AmazonRoute53 RecoveryControlConfigReadOnlyAccess | 18 de agosto de 2021 |
| O Route 53 ARC começou a monitorar alterações | O Route 53 ARC começou a rastrear as mudanças em suas políticas AWS gerenciadas. | 27 de julho de 2021 |

## Solução de problemas de identidade e acesso ao Controlador de recuperação de aplicação do Amazon Route 53

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Route 53 ARC e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Route 53 ARC
- Não estou autorizado a realizar iam: PassRole

- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos ARC do Route 53

## Não tenho autorização para executar uma ação no Route 53 ARC

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Seu administrador é a pessoa que forneceu suas credenciais de início de sessão.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um recurso do *`my-example-widget`* fictício, mas não tem as permissões fictícias do `route53-recovery-readiness:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 route53-recovery-readiness:GetWidget on resource: my-example-widget
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *`my-example-widget`* usando a ação `route53-recovery-readiness:`*`GetWidget`*.

## Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Route 53 ARC.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Route 53 ARC. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar a função para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

### Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos ARC do Route 53

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Route 53 ARC oferece suporte a esses atributos, consulte Como o Controlador de recuperação de aplicações do Amazon Route 53 funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

## Registro de chamadas e monitoramento da API do Controlador de recuperação de aplicações do Amazon Route 53

O monitoramento é uma parte importante da manutenção da disponibilidade e do desempenho do Amazon Route 53 Application Recovery Controller e 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. AWS fornece várias ferramentas para monitorar seus recursos e atividades do Route 53 ARC e responder a possíveis incidentes:

CloudWatch Métricas e alarmes da Amazon

Usando CloudWatch, você pode monitorar, em tempo real, seus AWS recursos e os aplicativos em que você executa AWS. CloudWatch coleta e rastreia métricas, que são variáveis que você mede ao longo do tempo. Você pode criar alarmes que monitoram métricas específicas e, em seguida, enviar notificações ou fazer alterações automaticamente nos recursos que você está monitorando quando a métrica exceder um determinado limite por um período de tempo. Para ter mais informações, consulte Usando a Amazon CloudWatch com o Route 53 ARC.

AWS CloudTrail troncos

CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Route 53 ARC. CloudTrailcaptura todas as chamadas de API para o Route 53 ARC como eventos, incluindo chamadas do console do Route 53 ARC e de chamadas de código para a API ARC do Route 53. Para ter mais informações, consulte Registrar chamadas da API do Route 53 ARC usando o AWS CloudTrail.

# Validação de conformidade do Controlador de recuperação de aplicações do Amazon Route 53

Auditores terceirizados avaliam a segurança e a conformidade do Amazon Route 53 Application Recovery Controller como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, HIPAA e outros.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.

- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

# Resiliência do Controlador de recuperação de aplicações do Amazon Route 53

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente

executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Route 53 ARC oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

# Infraestrutura de segurança do Controlador de recuperação de aplicações do Amazon Route 53

Como um serviço gerenciado, o Amazon Route 53 Application Recovery Controller é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Route 53 ARC pela rede. Os clientes precisam oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando 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.

# Exemplos de código para o Application Recovery Controller usando AWS SDKs

Os exemplos de código a seguir mostram como usar o Application Recovery Controller com um kit de desenvolvimento de AWS 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, consulteUsar o Route 53 ARC 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 Application Recovery Controller usando AWS SDKs
  - Obtenha o estado de um controle de roteamento do Application Recovery Controller usando um SDK AWS
  - Atualize o estado de um controle de roteamento do Application Recovery Controller usando um SDK AWS

## Ações para o Application Recovery Controller usando AWS SDKs

Os exemplos de código a seguir demonstram como realizar ações individuais do Application Recovery Controller com AWS SDKs. Esses trechos chamam a API do Controlador de recuperação de aplicações e são partes 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 Referência de API do Controlador de recuperação de aplicações de Amazon Route 53.

Exemplos

- Obtenha o estado de um controle de roteamento do Application Recovery Controller usando um SDK AWS

- Atualize o estado de um controle de roteamento do Application Recovery Controller usando um SDK AWS

## Obtenha o estado de um controle de roteamento do Application Recovery Controller usando um SDK AWS

Os exemplos de código a seguir mostram como obter o estado de um controle de roteamento do Controlador de recuperação de aplicativos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
    public static GetRoutingControlStateResponse
 getRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region())).build();
                return client.getRoutingControlState(
                        GetRoutingControlStateRequest.builder()
                                .routingControlArn(routingControlArn).build());
            } catch (Exception exception) {
```

```
                System.out.println(exception);
            }
        }
        return null;
    }
```

- Para obter detalhes da API, consulte GetRoutingControlStatea Referência AWS SDK for Java 2.x da API.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def get_routing_control_state(routing_control_arn, cluster_endpoints):
```

```
    """
    Gets the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.

    :param routing_control_arn: The ARN of the routing control to look up.
    :param cluster_endpoints: The list of cluster endpoints to query.
    :return: The routing control state response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.get_routing_control_state(
                RoutingControlArn=routing_control_arn
            )
            return response
        except Exception as error:
            print(error)
            raise error
```

- Para obter detalhes da API, consulte a GetRoutingControlStateReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o Route 53 ARC com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

## Atualize o estado de um controle de roteamento do Application Recovery Controller usando um SDK AWS

Os exemplos de código a seguir mostram como atualizar o estado de um controle de roteamento do Controlador de recuperação de aplicações.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
    public static UpdateRoutingControlStateResponse
 updateRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn,
            String routingControlState) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region()))
                        .build();
                return client.updateRoutingControlState(
                        UpdateRoutingControlStateRequest.builder()

 .routingControlArn(routingControlArn).routingControlState(routingControlState).build());
            } catch (Exception exception) {
                System.out.println(exception);
            }
        }
        return null;
    }
```

- Para obter detalhes da API, consulte UpdateRoutingControlStatea Referência AWS SDK for Java 2.x da API.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def update_routing_control_state(
    routing_control_arn, cluster_endpoints, routing_control_state
):
    """
    Updates the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.
```

```
    :param routing_control_arn: The ARN of the routing control to update the
 state for.
    :param cluster_endpoints: The list of cluster endpoints to try.
    :param routing_control_state: The new routing control state.
    :return: The routing control update response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.update_routing_control_state(
                RoutingControlArn=routing_control_arn,
                RoutingControlState=routing_control_state,
            )
            return response
        except Exception as error:
            print(error)
```

- Para obter detalhes da API, consulte a UpdateRoutingControlStateReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o Route 53 ARC com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

# Cotas no Controlador de recuperação de aplicações do Amazon Route 53

O Controlador de recuperação de aplicações do Amazon Route 53 está sujeito às seguintes cotas (anteriormente chamadas de limites).

## Cotas para verificação de prontidão do ARC do Route 53

| Entidade | Quota |
|---|---|
| Número de grupos de recuperação por conta | 5 |
| Número de células por conta | 15 |
| Número de células aninhadas por célula | 3 |
| Número de células por grupo de recuperação | 3 |
| Número de recursos por célula | 10 |
| Número de recursos por grupo de recuperação | 10 |
| Número de recursos por conjunto de recursos | 6 |
| Número de conjuntos de recursos por conta | 200 |
| Número de verificações de prontidão por conta | 200 |
| Número de autorizações entre contas | 100 |

## Cotas para controle de roteamento do ARC do Route 53

| Entidade | Quota |
|---|---|
| Número de clusters por conta | 2 |
| Número de painéis de controle por cluster | 50 |

| Entidade | Quota |
| --- | --- |
| Número de controles de roteamento por painel de controle. | 100 |
| Número total de controles de roteamento (em todos os painéis de controle) por cluster | 300 |
| Número de regras de segurança por painel de controle | 20 |
| Número de controles de roteamento por chamada de operação Atualizar estado de controle de roteamento | 10 |
| Número de chamadas de API de mudança para um endpoint de cluster, por segundo | 3 |

# Informações do Controlador de Recuperação de Aplicações do Amazon Route 53

As informações e os recursos listados aqui podem ajudar você a saber mais sobre o Controlador de Recuperação de Aplicações Amazon Route 53.

Tópicos



## Documentação adicional do Controlador de Recuperação de Aplicações Amazon Route 53

Os seguintes recursos relacionados podem ajudá-lo enquanto você trabalha com o ARC do Route 53.

- Guia de referência da API do Controlador de Recuperação de Aplicações Amazon Route 53: fornece descrições completas das ações da API, parâmetros e tipos de dados, e uma lista de erros para preparação da recuperação.
- Guia de referência de configuração da API de controle de recuperação do Controlador de Recuperação de Aplicações Amazon Route 53: fornece descrições completas das ações da API, parâmetros e tipos de dados, e uma lista de erros da configuração do controle de recuperação.
- Guia de referência da API de controle de roteamento do Controlador de Recuperação de Aplicações Amazon Route 53: fornece descrições completas das ações, parâmetros e tipos de dados da API, e uma lista de erros do controle de roteamento.
- Informações sobre o produto ARC do Route 53: a principal página para obter informações sobre o Route 53, incluindo recursos e benefícios.
- Informações sobre preços do ARC do Route 53: detalhes sobre preços.
- Termos de uso: informações detalhadas sobre nossos direitos autorais e marca registrada, sua conta, licença e acesso ao site, entre outros tópicos.

# Obter suporte

O suporte para o ARC do Route 53 está disponível de várias formas.

- Atendimento ao cliente AWS Support: este site reúne informações sobre casos de suporte e resultados recentes do AWS Trusted Advisor e de verificações de integridade, além de links para fóruns de discussão, perguntas técnicas frequentes, o painel de integridade do serviço e informações sobre os planos do AWS Support.
- 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.

# Dicas do blog da Amazon Web Services

O blog da AWS tem vários posts para ajudar você a usar os serviços da AWS. Por exemplo, consulte os seguintes posts do blog sobre o Controlador de Recuperação de Aplicações Amazon Route 53:

- Para saber mais sobre como usar o AWS Resource Access Manager com o Controlador de Recuperação de Aplicações do Amazon Route 53 para suporte entre contas, consulte a seguinte postagem do blog: Cross-account support in Amazon Route 53 Application Recovery Controller.
- Para saber mais sobre a criação de serviços tolerantes a falhas usando zonas de disponibilidade (AZs) para se recuperar mais facilmente de falhas graves e falhas cinzentas, inclusive iniciando uma mudança de zona, consulte a seguinte postagem do blog: Rapidly recover from application failures in a single AZ.
- Para saber mais sobre abordagens para mitigar falhas e depois retornar às operações normais com o Route 53, incluindo o uso do ARC do Route 53, consulte a seguinte publicação no blog AWS News: Criação de mecanismos de recuperação de desastres usando o Amazon Route 53.
- Para saber mais sobre a criação de uma aplicação de pilha de região única altamente resiliente com o Route 53 ARC, consulte a seguinte publicação do blog (primeira parte de uma série): Building highly resilient applications using Amazon Route 53 Application Recovery Controller, Part 1: Single-Region stack.
- Para saber mais sobre a criação de uma aplicação de pilha multirregional altamente resiliente com o Route 53 ARC, consulte a seguinte publicação do blog (segunda parte de uma série): Building

highly resilient applications using Amazon Route 53 Application Recovery Controller, Part 2: Multi-Region stack.

- Para saber mais sobre como usar o Route 53 ARC e baixar o modelo Hashicorp Terraform para ajudar você a começar, consulte a seguinte publicação do blog: Running recovery-oriented applications with Amazon Route 53 Application Recovery Controller, AWS CI/CD tools, and Terraform.
- Para saber mais sobre como usar o ARC do Route 53 e baixar um modelo do AWS CloudFormation para ajudar você a começar, consulte a seguinte publicação no blog AWS News: Simplifique a recuperação com o ARC do Route 53.

# Histórico do documento do Guia do desenvolvedor do Controlador de recuperação de aplicações do Amazon Route 53

As entradas a seguir descrevem alterações importantes feitas na documentação do Controlador de recuperação de aplicações do Amazon Route 53.

- Versão: mais recente
- Última atualização da documentação: 30 de novembro de 2023

| Alteração | Descrição | Data |
| --- | --- | --- |
| Adiciona o recurso de mudança automática de zona | Adiciona um novo recurso no Route 53 ARC, no qual você autoriza a AWS a transferir o tráfego de recursos de uma aplicação para fora de uma zona de disponibilidade, em seu nome, para ajudar a reduzir o tempo de recuperação durante eventos.<br><br>Para obter mais informações, consulte Zonal autoshift in Amazon Route 53 Application Recovery Controller. | 30 de novembro de 2023 |
| Adiciona um novo perfil vinculado ao serviço | Adiciona um novo perfil vinculado ao serviço, AWSServiceRoleForZonalAutoshiftPracticeRun, para execuções práticas de mudança automática de zona. | 30 de novembro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | Para obter mais informações, consulte Service-linked role permissions for AWSServiceRoleForZonalAutoshiftPracticeRun. | |
| Adiciona compatibilidade abrangendo todas as contas com clusters | Adiciona suporte entre contas para clusters no Route 53 ARC com AWS Resource Access Manager, para que você possa usar um cluster com facilidade e segurança, hospedar painéis de controle e controles de roteamento pertencentes a várias contas diferentes da AWS.<br><br>Para obter mais informações, consulte Suporte entre contas para clusters no Route 53 ARC. | 18 de outubro de 2023 |
| Política gerenciada atualizada | Atualiza a política gerenciada `AmazonRoute53RecoveryControlConfigReadOnly` para adicionar permissões para `GetResourcePolicy` e oferecer suporte ao retorno de detalhes sobre políticas AWS Resource Access Manager de recursos para recursos compartilhados.<br><br>Para obter mais informações, consulte Políticas gerenciadas da AWS. | 19 de setembro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Atualização do perfil vinculado ao serviço | Adição de novas permissões, `ec2:DescribeVpnGateways` e `ec2:DescribeCustomerGateways`, ao perfil vinculado ao serviço do Route 53 ARC, para oferecer suporte à pesquisa de instâncias do Amazon EC2.<br><br>Para obter mais informações, consulte Usar perfis vinculados a serviços para o Route 53 ARC. | 17 de fevereiro de 2023 |
| Versão GA para mudança de zona | Suporta a versão GA da mudança de zona para o Route 53 ARC, que inclui controle de acesso por atributo (ABAC) para recursos gerenciados registrados no Route 53 ARC para mudança de zona.<br><br>Para obter mais informações, consulte Controle de acesso por atributo (ABAC) com o Route 53 ARC. | 10 de janeiro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Foi adicionada uma nova mudança de zona Multi-AZ | Foi adicionado conteúdo descrevendo um novo serviço no Route 53 ARC, mudança de zona, para aplicativos Multi-AZ. É possível iniciar uma mudança de zona para mover temporariamente o tráfego de um recurso do balanceador de carga para fora de uma zona de disponibilidade.<br><br>Para obter mais informações, consulte Mudança de zona no Route 53 ARC. | 28 de novembro de 2022 |
| Atualização do perfil vinculado ao serviço | Adição de uma nova permissão, `lambda:ListProvisionedConcurrencyConfigs` , ao perfil vinculado ao serviço do Route 53 ARC para consultar informações sobre as funções do Lambda.<br><br>Para obter mais informações, consulte Usar perfis vinculados a serviços para o Route 53 ARC. | 31 de agosto de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Política gerenciada atualizada | Atualizou a política gerenciada `AmazonRoute53RecoveryControlConfigFullAccess` para remover as permissões do Amazon Route 53 e listá-las como opcionais.<br><br>Para obter mais informações, consulte Políticas gerenciadas da AWS para o Controlador de recuperação de aplicações do Amazon Route 53. | 26 de maio de 2022 |
| Política gerenciada atualizada | Atualizou a política gerenciada `AmazonRoute53RecoveryControlConfigFullAccess` para incluir as permissões necessárias do Amazon Route 53.<br><br>Para obter mais informações, consulte Políticas gerenciadas da AWS para o Controlador de recuperação de aplicações do Amazon Route 53. | 15 de abril de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Exemplo de CLI adicionado para a nova API de listas de controles de roteamento | Foram adicionados exemplos de comandos CLI e recomendações de melhores práticas para a nova operação da API de listas de controles de roteamento incluída na API de plano de dados extremamente confiável do Route 53 ARC.<br><br>Para obter mais informações, consulte Listar e atualizar controles e estados de roteamento. | 31 de março de 2022 |
| Adicionado o suporte para sobrepor regras de segurança | Foi adicionado suporte para sobrepor as regras de segurança, o que permite ignorar as proteções de controle de roteamento aplicadas com as regras de segurança configuradas. A sobreposição das regras de segurança pode ser necessária, por exemplo, em um cenário de emergência durante o failover para recuperação de desastres.<br><br>Para obter mais informações, consulte Sobrepor regras de segurança para redirecionar o tráfego. | 2 de março de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Agregado suporte adicional de marcação | Foi adicionado suporte para marcar recursos adicionais no Route 53 ARC, incluindo clusters, painéis de controle, controles de roteamento e regras de segurança.<br><br>Para obter mais informaçõ es, consulte Marcações no desenvolvedor do Controlador de recuperação de aplicações do Amazon Route 53. | 20 de dezembro de 2021 |
| Política gerenciada atualizada | A política gerenciada `AmazonRoute53Recov eryControlConfigRe adOnly` foi atualizada para adicionar permissão para listar as tags de um recurso.<br><br>Para obter mais informações, consulte Políticas gerenciadas da AWS para o Controlador de recuperação de aplicações do Amazon Route 53. | 20 de dezembro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Adicionado o suporte para alertas em tempo real com o EventBridge | Foi adicionado suporte para o EventBridge, o que significa que agora você pode adicionar regras para receber alertas e agir de acordo com as mudanças de status da verificação de prontidão do Route 53 ARC, por exemplo, quando um status muda de PRONTO para NÃO PRONTO.<br><br>Para mais informações, consulte Usar o Route 53 ARC com o Amazon EventBridge. | 20 de dezembro de 2021 |
| Exemplos de código de estado de controle de roteamento adicionados | Amostras de código adicionadas para ilustrar como testar endpoints de cluster em sequência ao usar operações de API para obter ou atualizar estados de controle de roteamento.<br><br>Para obter mais informações, consulte Exemplos de API do Controlador de recuperação de aplicações do Amazon Route 53. | 16 de novembro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Adicionadas novas permissões para a política de somente de leitura | Adicionadas duas novas permissões à política `AmazonRoute53RecoveryReadinessReadOnlyAccess` : `route53-recovery-readiness:GetArchitectureRecommendations` e `route53-recovery-readiness:GetCellReadinessSummary` .<br><br>Para obter mais informações, consulte Políticas gerenciadas da AWS para o Controlador de recuperação de aplicações do Amazon Route 53. | 9 de novembro de 2021 |
| Adicionado suporte para o tipo de recurso do Amazon API Gateway. | Adicionou um novo tipo de recurso, Amazon API Gateway, e atualizou as permissões de função vinculadas ao serviço Route 53 ARC para que ele audite o API Gateway com verificações de prontidão.<br><br>Para obter mais informações, consulte Regras de prontidão e tipos de recursos suportados e Uso de funções vinculadas a serviços para o Route 53 ARC. | 28 de outubro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Foi adicionado suporte para o tipo de recurso de funções do Lambda | Adicionou um novo tipo de recurso, função do Lambda, e atualizou as permissões de função vinculadas ao serviço Route 53 ARC para que ele audite funções do Lambda com verificações de prontidão.<br><br>Para obter mais informações, consulte Regras de prontidão e tipos de recursos suportados e Uso de funções vinculadas a serviços para o Route 53 ARC. | 8 de outubro de 2021 |
| Links adicionados aos modelos CloudFormation e Terraform | Links adicionados para download no AWS CloudFormation e modelos do Hashicorp Terraform para ajudar você a começar a usar rapidamente o Route 53 ARC. Para obter mais informações, consulte Preparação para recuperação com um novo aplicativo. | 13 de setembro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Novas políticas gerenciadas adicionada | Foram adicionadas as seguintes políticas gerenciadas da AWS para o Route 53 ARC: `AmazonRoute53RecoveryReadinessFullAccess`, `AmazonRoute53RecoveryReadinessReadOnlyAccess`, `AmazonRoute53RecoveryClusterFullAccess`, `AmazonRoute53RecoveryClusterReadOnlyAccess`, `AmazonRoute53RecoveryControlConfigFullAccess`, e `AmazonRoute53RecoveryControlConfigReadOnlyAccess`.<br><br>Para obter mais informações, consulte Políticas gerenciadas da AWS para o Controlador de recuperação de aplicações do Amazon Route 53. | 18 de agosto de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Iniciado o rastreamento de políticas gerenciadas da AWS para o Controlador de recuperação de aplicações do Amazon Route 53 | As atualizações das políticas gerenciadas serão monitoradas a partir da data de lançamento inicial.<br><br>Para obter mais informações, consulte Políticas gerenciadas da AWS para o Controlador de recuperação de aplicações do Amazon Route 53. | 27 de julho de 2021 |
| Versão inicial do Controlador de recuperação de aplicações do Amazon Route 53. | O Route 53 ARC melhora a disponibilidade dos aplicativos ao coordenar centralmente os failovers em uma região da AWS ou em várias regiões. O Route 53 ARC fornece verificações de prontidão para garantir que seus aplicativos sejam escalados para lidar com o tráfego de failover e configurados para contornar falhas. Ele também fornece controle de roteamento extremamente confiável para que você possa recuperar aplicativos redirecionando o tráfego, por exemplo, entre zonas de disponibilidade ou regiões. Para mais informações, consulte O que é o Route 53 ARC?. | 27 de julho de 2021 |

# 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.