aws

Guia do Desenvolvedor

Amazon Application Recovery Controller (ARC)

Amazon Application Recovery Controller (ARC): Guia do Desenvolvedor

Table of Contents

O que é ARC?

O Amazon Application Recovery Controller (ARC) ajuda você a se preparar e concluir uma recuperação mais rápida de aplicativos executados na infraestrutura de nuvem AWS global.

O ARC fornece os seguintes recursos:

- Recuperação de zona de disponibilidade múltipla (AZ), incluindo mudança zonal e mudança automática zonal, que permitem que você se recupere de deficiências únicas de AZ transferindo temporariamente o tráfego de uma AZ prejudicada para uma AZ saudável.
- Recuperação multirregional, que inclui controle de roteamento para failover e verificação de prontidão para monitoramento de aplicativos.

Recuperação de várias zonas de disponibilidade

Mudança de zona

Você pode usar o deslocamento zonal ARC para isolar e se recuperar rapidamente de deficiências em uma única Zona de Disponibilidade (AZ). A mudança de zona transfere temporariamente o tráfego de um recurso suportado de uma AZ deficiente para um estado saudável AZs na mesma AWS região. 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 AWS deficiência em uma única AZ. Desviar o tráfego da AZ prejudicada reduz o impacto para os clientes que estão usando seu aplicativo na AZ prejudicada.

Você pode iniciar uma mudança de zona para qualquer recurso suportado em sua conta em uma AWS região. Os turnos zonais são manuais e temporários. Ao iniciar uma mudança zonal, você deve especificar uma expiração (prorrogável) de até três dias. Para habilitar a mudança de zona para os recursos suportados, consulte. Recursos compatíveis

Mudança automática zonal

O deslocamento automático zonal do ARC AWS autoriza a transferência do tráfego de uma AZ prejudicada para recursos suportados, em seu nome, para um tráfego saudável AZs na mesma região. AWS AWS inicia uma mudança automática zonal quando a telemetria interna indica que há uma deficiência em uma AZ em uma AWS região que pode potencialmente afetar os clientes. A telemetria interna incorpora métricas de várias fontes, incluindo a AWS rede e os serviços Amazon EC2 e Elastic Load Balancing.

As mudanças automáticas zonais são temporárias. AWS encerra um deslocamento automático zonal quando os indicadores de telemetria internos mostram que não há mais um problema ou um problema potencial.

Para saber mais sobre esses recursos, consulte os seguintes capítulos:

- Mudança zonal no ARC
- Mudança automática zonal em ARC

Recuperação multirregional

Controle de roteamento

Os controles de roteamento extremamente confiáveis do ARC permitem a recuperação em várias regiões para que seus aplicativos possam fazer o failover do tráfego DNS do Sistema de Nomes de Domínio em todas as regiões. AWS

Se seu aplicativo foi projetado para operar em várias AWS regiões, você pode usar o controle de roteamento ARC para realizar o failover entre regiões. O controle de roteamento permite que você transfira o tráfego de uma AWS região com problemas para uma AWS região saudável, para que você possa garantir que seu aplicativo mantenha a disponibilidade. O controle de roteamento inclui regras de segurança, que ajudam a protegê-lo de resultados não intencionais ao impor grades de proteção definidas por você. Por exemplo, você pode impor uma regra de segurança de que somente uma das réplicas do seu aplicativo, ativa ou em espera, esteja ativada e em uso.

Verificação de prontidão

A verificação de prontidão do ARC monitora continuamente as cotas de AWS recursos, a capacidade e as políticas de roteamento de rede e pode notificá-lo sobre alterações que podem afetar sua capacidade de fazer o failover para um aplicativo de réplica e se recuperar de uma deficiência na região. As verificações contínuas de prontidão garantem que você possa manter seus aplicativos multirregionais em um estado dimensionado e configurado para lidar com o tráfego de failover. A verificação de prontidão é útil quando você configura o ARC pela primeira vez e durante a operação normal do aplicativo. A verificação de prontidão não deve ser usada no caminho crítico de failover durante um evento.

Para saber mais sobre esses recursos, consulte os seguintes capítulos:

- Controle de roteamento no ARC

- Verificação de prontidão no ARC

Compare os recursos de recuperação multi-AZ e multirregional no ARC

A mudança zonal, a mudança automática zonal e o controle de roteamento no Amazon Application Recovery Controller (ARC) podem alcançar uma recuperação rápida e ajudar você a garantir a resiliência de seus aplicativos. AWS Esses recursos são altamente disponíveis e ajudam a apoiar a recuperação em cenários em que seu aplicativo está experimentando maior latência ou disponibilidade reduzida. Esses recursos também ajudam a recuperar aplicativos rapidamente, afastando o tráfego de deficiências isoladas, o que limita o impacto e o tempo perdido com as deficiências.

O controle de roteamento se concentra principalmente em AWS aplicativos que estão em várias AWS regiões (multirregião), enquanto o deslocamento zonal e o deslocamento automático zonal suportam apenas o deslocamento de tráfego para recursos compatíveis com aplicativos Multi-AZ.

As informações na tabela a seguir incluem alguns dos principais recursos do deslocamento zonal, do deslocamento automático zonal e do controle de roteamento. Essas descrições podem ajudar você a entender melhor como uma opção específica pode ser a melhor opção para as necessidades do aplicativo.

Controle de roteamento	Mudança de zona	Mudança automática de zona
Regional	De zona	De zona
Redireciona o tráfego de uma AWS região para outra (principalmente)	Desvia o tráfego de uma zona de disponibilidade	Desvia o tráfego de uma zona de disponibilidade
	O tráfego vai para outras zonas de disponibilidade na região, não para um destino específico	O tráfego vai para outras zonas de disponibilidade na região, não para um destino específico
Requer configuração	Pode exigir configuração	Requer configuração
Requer configuração e setup	Requer a aceitação de alguns recursos compatíveis	Deve estar habilitado para um recurso compatível

Controle de roteamento	Mudança de zona	Mudança automática de zona
	Para obter mais informações, consulte Recursos compatíveis	Para obter mais informações, consulte Recursos compatíveis
Iniciada pelo cliente O cliente determina quando redirecionar o tráfego	Iniciada pelo cliente O cliente determina quando iniciar uma mudança de zona	Iniciada pela AWS AWS afasta o tráfego do aplicativo de uma AZ em seu nome
Com base em taxas Requer cobranças separadas para controle de roteamento	Incluído nos serviços (sem custo adicional) A criação de mudanças zonais para afastar o tráfego AZs está incluída nos recursos suportados.	Incluído nos serviços (sem custo adicional) Iniciar turnos automáticos para afastar o tráfego AZs em seu nome está incluído nos recursos suportados.
Não expira O tráfego pode ser redirecionado para uma réplica indefinidamente	Temporária Todas as mudanças de zona devem ser configuradas para expirar	Temporária AWS inicia e termina os turnos automáticos

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

- Mudança zonal no ARC
- Mudança automática zonal em ARC
- Controle de roteamento no ARC

Use o deslocamento zonal e o deslocamento automático zonal para recuperar aplicativos no ARC

Esta seção explica como usar os recursos do Amazon Application Recovery Controller (ARC) para recuperar de forma confiável seu AWS recurso de um problema em uma zona de disponibilidade (AZ) comprometida. A mudança zonal e a mudança automática zonal afastam temporariamente o tráfego de um recurso suportado de um AZ danificado, o que reduz o tempo de recuperação de seus aplicativos.

A principal diferença entre mudança zonal e mudança automática zonal é que uma é uma mudança de tráfego manual que você controla, e a outra afasta automaticamente o tráfego de uma deficiência em seu nome.

- Com a mudança zonal, você transfere manualmente o tráfego de um recurso suportado para Região da AWS fora de uma zona de disponibilidade.
- Com o deslocamento automático zonal, o tráfego de um recurso suportado é automaticamente transferido de um AZ danificado e redirecionado para íntegro na mesma região. AZs AWS

Os tópicos a seguir descrevem os recursos de mudança zonal e de mudança automática zonal e como usá-los.

Tópicos

Mudança zonal no ARC

A mudança de zona do Amazon Application Recovery Controller (ARC) permite que você transfira o tráfego de um recurso suportado de uma Zona de Disponibilidade (AZ) comprometida Região da AWS para um saudável AZs na mesma região. Retirar o tráfego do seu recurso de uma AZ prejudicada reduz a duração e a gravidade do impacto causado por quedas de energia ou problemas de hardware ou software em uma AZ, além de ajudar a mitigar problemas e recuperar rapidamente seu aplicativo. Você pode optar por mudar o tráfego, por exemplo, porque uma implantação ruim está causando problemas de latência ou porque a Availability Zone está afetada.

Você deve optar por recursos para usar o deslocamento zonal. Para obter mais informações, consulte Recursos compatíveis.

Antes de iniciar uma mudança de zona, você deve pré-escalar seu aplicativo e garantir que tenha capacidade suficiente para retirar o tráfego de uma zona de disponibilidade. Depois de pré-escalar, você pode escolher a zona de disponibilidade da qual se afastar e o recurso para o qual transferir o tráfego e, em seguida, iniciar a mudança zonal. Você pode cancelar o turno a qualquer momento para que o tráfego comece a retornar à zona de disponibilidade original. Para obter mais informações, consulte Práticas recomendadas para mudanças de zona no ARC.

Todas as mudanças zonais são mitigações temporárias. Você define uma expiração inicial ao iniciar uma mudança de zona, de um minuto a três dias (72 horas), que pode ser estendida se precisar continuar a mudança de tráfego.

Em cenários específicos, a mudança zonal não afasta o tráfego do AZ. Para obter mais informações, consulte Recursos compatíveis.

Como funciona uma mudança de zona

Quando você inicia uma mudança de zona para um recurso compatível, o tráfego do recurso é removido da Zona de Disponibilidade (AZ) que você especificou. Os recursos suportados pelo ARC fornecem integrações que marcam a AZ especificada como não íntegra, o que resulta no afastamento do tráfego da AZ prejudicada.

O tráfego começa a mudar - Quando você inicia uma mudança de zona no ARC, talvez não veja o tráfego sair da Zona de Disponibilidade imediatamente. Pode levar pouco 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. As configurações de DNS e outros fatores, incluindo conexões existentes, podem ser concluídas em apenas alguns minutos, mas podem levar mais tempo. Para obter mais informações, consulte Garantir que os turnos de trânsito terminem rapidamente.

A mudança de tráfego termina - Quando uma mudança de zona expira ou você a cancela, o ARC toma medidas para interromper a mudança de tráfego e reverte o processo de iniciar uma mudança de tráfego. Agora, a AZ recuperada é reconhecida como disponível para o recurso e o tráfego continua fluindo para a AZ.

Você deve definir que todos os turnos zonais expirem quando você iniciar os turnos. 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.

Quando o tráfego não se afasta — Em cenários específicos, uma mudança de zona não desvia o tráfego da Zona de Disponibilidade. Por exemplo, digamos que você inicia uma mudança de zona para um balanceador de carga quando os grupos-alvo do balanceador de carga AZs não têm nenhuma instância ou se todas as instâncias não estão íntegras. Nesse cenário, o balanceador de carga está em um estado de falha aberta e o início de uma mudança de zona não afasta o tráfego.

Antes de iniciar uma mudança zonal para um recurso, verifique se todas as condições para uma mudança zonal bem-sucedida foram atendidas. AWS os recursos lidam com as mudanças zonais de forma diferente. Para obter mais informações sobre o suporte a mudanças de zona, consulte Recursos compatíveis.

Região da AWS disponibilidade para mudança zonal

Para obter informações detalhadas sobre endpoints regionais de suporte e serviço para o Amazon Application Recovery Controller (ARC), consulte os endpoints e cotas do Amazon Application Recovery Controller (ARC) na Referência geral da Amazon Web Services.

Atualmente, o deslocamento zonal e o deslocamento automático zonal estão disponíveis na Regiões da AWS lista aqui. A mudança zonal e a mudança automática zonal também estão disponíveis nas regiões da China, ou seja, na região da China (Pequim) e na região da China (Ningxia). Os recursos que usam o Amazon Application Recovery Controller (ARC) podem ter considerações adicionais. Para obter mais informações, consulte Recursos compatíveis.

Nome da região	Região	Endpoint	Protocolo	
Leste dos EUA (Ohio)	us-east-2	arc-zonal-shift.us-east-2.amazonaws.com	HTTPS	
		arc-zonal-shift-fips.us-east-2.api.aws	HTTPS	
		arc-zonal-shift.us-east-2.api.aws	HTTPS	
Leste dos EUA (Norte da Virgínia)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS	
		arc-zonal-shift-fips.us-east-1.api.aws	HTTPS	
		arc-zonal-shift.us-east-1.api.aws	HTTPS	

Nome da região	Região	Endpoint	Protocolo
Oeste dos EUA (N. da Califórnia)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-1.api.aws	HTTPS
		arc-zonal-shift.us-west-1.api.aws	HTTPS
Oeste dos EUA (Oregon)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-2.api.aws	HTTPS
		arc-zonal-shift.us-west-2.api.aws	HTTPS
África (Cidade do Cabo)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.af-south-1.api.aws	HTTPS
Ásia-Pacífico (Hong Kong)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-east-1.api.aws	HTTPS
Ásia-Pacífico (Hyderabad)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-south-2.api.aws	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-3.api.aws	HTTPS
Ásia-Pacífico (Malásia)	ap-southeast-5	arc-zonal-shift.ap-southeast-5.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-5.api.aws	HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Melbourne)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com arc-zonal-shift.ap-southeast-4.api.aws	HTTPS HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com arc-zonal-shift.ap-south-1.api.aws	HTTPS HTTPS
Ásia-Pacífico (Osaka)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com arc-zonal-shift.ap-northeast-3.api.aws	HTTPS HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com arc-zonal-shift.ap-northeast-2.api.aws	HTTPS HTTPS
Ásia-Pacífico (Singapura)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com arc-zonal-shift.ap-southeast-1.api.aws	HTTPS HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com arc-zonal-shift.ap-southeast-2.api.aws	HTTPS HTTPS
Ásia-Pacífico (Taipei)	ap-east-2	arc-zonal-shift.ap-east-2.amazonaws.com arc-zonal-shift.ap-east-2.api.aws	HTTPS HTTPS
Ásia-Pacífico (Tailândia)	ap-southeast-7	arc-zonal-shift.ap-southeast-7.amazonaws.com arc-zonal-shift.ap-southeast-7.api.aws	HTTPS HTTPS

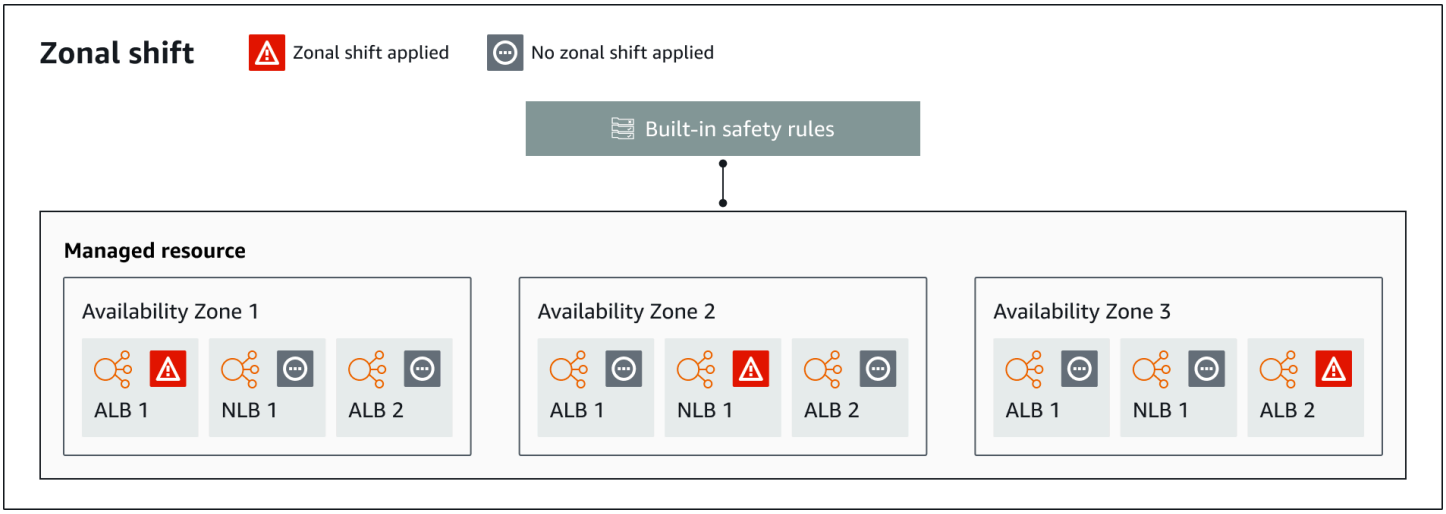
Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Tóquio)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-northeast-1.api.aws	HTTPS
Canadá (Central)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-central-1.api.aws	HTTPS
		arc-zonal-shift.ca-central-1.api.aws	HTTPS
Oeste do Canadá (Calgary)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-west-1.api.aws	HTTPS
		arc-zonal-shift.ca-west-1.api.aws	HTTPS
Europa (Frankfurt)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-central-1.api.aws	HTTPS
Europa (Irlanda)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-1.api.aws	HTTPS
Europa (Londres)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-2.api.aws	HTTPS
Europa (Milão)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-south-1.api.aws	HTTPS
Europa (Paris)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-3.api.aws	HTTPS
Europa (Espanha)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-south-2.api.aws	HTTPS

Nome da região	Região	Endpoint	Protocolo
Europa (Estocolmo)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-north-1.api.aws	HTTPS
Europa (Zurique)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-central-2.api.aws	HTTPS
Israel (Tel Aviv)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.il-central-1.api.aws	HTTPS
México (Central)	mx-central-1	arc-zonal-shift.mx-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.mx-central-1.api.aws	HTTPS
Oriente Médio (Barém)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.me-south-1.api.aws	HTTPS
Oriente Médio (Emirados Árabes Unidos)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.me-central-1.api.aws	HTTPS
América do Sul (São Paulo)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com	HTTPS
		arc-zonal-shift.sa-east-1.api.aws	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-gov-east-1.api.aws	HTTPS
		arc-zonal-shift.us-gov-east-1.api.aws	HTTPS

Nome da região	Região	Endpoint	Protocolo
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-gov-west-1.api.aws	HTTPS
		arc-zonal-shift.us-gov-west-1.api.aws	HTTPS

Componentes da mudança de zona

O diagrama a seguir ilustra um exemplo de uma mudança zonal deslocando o tráfego de uma zona de disponibilidade em um. Região da AWS As verificações incorporadas à mudança zonal evitam que você inicie outra mudança zonal para um recurso quando ele já tem uma mudança ativa.



A seguir estão os componentes da capacidade de mudança zonal no ARC.

Mudança de zona

> Você inicia uma mudança de zona de um recurso gerenciado em sua AWS conta para mover temporariamente o tráfego de uma zona de disponibilidade em uma zona de disponibilidade em uma Região da AWS, para saudável AZs na região, para se recuperar rapidamente de um problema em uma AZ. Para obter mais informações sobre os recursos suportados para mudança zonal, consulte. Recursos compatíveis

Verificações de segurança integradas

As verificações incorporadas ao ARC evitam que mais de uma mudança de tráfego para um recurso entre em vigor ao mesmo tempo. Ou seja, somente uma mudança de zona, execução prática ou mudança automática iniciada pelo cliente para o recurso pode estar ativamente afastando o tráfego 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 zonal em ARC 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).

Para uma mudança de zona, você só pode escolher recursos em sua conta para um AWS serviço que seja suportado pelo ARC. Para obter mais informações sobre os recursos suportados para mudança zonal, consulte. Recursos compatíveis

Atributos gerenciados

Alguns AWS recursos devem optar manualmente pela mudança de zona, e outros são ativados automaticamente. Para obter mais informações sobre os recursos suportados para mudança zonal, consulte. Recursos compatíveis

Nome do recurso

O nome de um recurso no ARC que você pode especificar para uma mudança de zona.

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 está em vigor para um recurso. A mudança que tem o status `APPLIED` determina a zona de disponibilidade em que o tráfego do aplicativo foi transferido para um recurso e quando essa mudança termina.

Tipo de turno

Define o tipo de deslocamento zonal. O `shiftType` pode ter os seguintes valores:

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- PRACTICE_RUN
- EXPERIMENTO FIS_

Tempo de expiração

O tempo de expiração para uma mudança de zona. As mudanças de zona são temporárias. Para uma mudança zonal, você pode inicialmente definir uma mudança zonal para ficar ativa por até três dias (72 horas).

Ao iniciar uma mudança zonal, você especifica por quanto tempo deseja que ela fique ativa, o que o ARC converte em um tempo de expiração (tempo de expiração). Você pode cancelar uma mudança de zona, por exemplo, se estiver 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 execuções práticas de mudança zonal que fazem parte da mudança automática zonal.

Planos de dados e controle para mudança zonal

Ao planejar o failover e a recuperação de desastres, considere a resiliência de seus mecanismos de failover. Recomendamos que você certifique-se de que os mecanismos dos quais você depende durante o failover estejam altamente disponíveis, para que você possa usá-los quando precisar deles em um cenário de desastre. Normalmente, você deve usar funções de plano de dados para seus mecanismos sempre que possível, 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 ambientes de gerenciamento e planos de dados e quando você pode confiar em uma expectativa de extrema confiabilidade com o plano de dados de um serviço.

Como acontece com a maioria dos AWS serviços, a funcionalidade da capacidade de mudança zonal é suportada por planos de controle e planos de dados. Embora ambos tenham sido criados para serem confiáveis, um plano de controle é otimizado para consistência de dados, enquanto um plano de dados é otimizado para disponibilidade. Um plano de dados é projetado para ser resistente e

manter a disponibilidade mesmo durante eventos de ruptura, quando um ambiente de gerenciamento pode ficar indisponível.

Em geral, um ambiente de gerenciamento 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 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.

Preços para mudança zonal no ARC

Para a mudança zonal, você pode iniciar uma mudança zonal para recursos suportados, para recuperar seu aplicativo de um problema em uma zona de disponibilidade. Não há cobrança adicional pelo uso da mudança de zona.

Para obter informações detalhadas sobre preços do ARC e exemplos de preços, consulte Preços do ARC.

Práticas recomendadas para mudanças de zona no ARC

Recomendamos as seguintes melhores práticas para usar mudanças zonais para recuperação Multi-AZ no ARC.

Tópicos

- Planejamento de capacidade e pré-escalabilidade
- Limite o tempo em que os clientes permanecem conectados aos seus endpoints
- Teste o início dos turnos zonais, com antecedência
- Garanta que todas as zonas de disponibilidade estejam saudáveis e recebam tráfego
- Use operações de API de plano de dados para recuperação de desastres
- Mova o tráfego com uma mudança de zona apenas temporariamente

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 recurso compatível e o tráfego é transferido de uma AZ, a capacidade que seu aplicativo estava usando para atender às solicitações é removida. Você deve garantir que tenha planejado uma transferência de tráfego para fora de uma AZ e possa continuar atendendo às solicitações restantes AZs.

Limite o tempo em que os clientes permanecem conectados aos seus endpoints

Quando o Amazon Application Recovery Controller (ARC) afasta o tráfego de uma deficiência, por exemplo, usando a mudança zonal ou a mudança automática zonal, o mecanismo que o ARC usa para mover o tráfego do seu aplicativo é uma atualização de DNS. Uma atualização de DNS faz com que todas as novas conexões sejam direcionadas para fora do local danificado.

No entanto, clientes com conexões abertas preexistentes podem continuar fazendo solicitações no local danificado até que os clientes se reconectem. Para garantir uma recuperação rápida, recomendamos que você limite a quantidade de tempo que os clientes permanecem conectados aos seus endpoints.

Teste o início dos turnos zonais, 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 recursos em 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. As vantagens dessa abordagem são que ela pode ser mais representativa da experiência de seus usuários finais e também reduz o risco de seu aplicativo e seu monitoramento serem afetados pelo mesmo desastre ao mesmo tempo.

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 API AWS Command Line Interface ou com ações de mudança de zona, com credenciais pré-armazenadas, se possível. Você também pode iniciar mudanças zonais 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.

Operações de API de mudança de zona

A tabela a seguir lista as operações da API ARC que você pode usar usando a mudança zonal, que afasta o tráfego de uma zona de disponibilidade para aplicativos 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 Exemplos de uso do AWS CLI com mudança zonal.

Ação	Usando o console ARC	Usando a API ARC
Iniciar uma mudança de zona	Consulte Iniciar uma mudança de zona	Consulte StartZonalShift
Atualizar uma mudança de zona	Consulte Atualizar ou cancelar uma mudança de zona	Consulte UpdateZonalShift
Listar mudanças de zona	Consulte Mudança zonal no ARC	Consulte ListZonalShifts
Listar recursos gerenciados	Consulte Recursos compatíveis	Consulte ListManagedResources

Ação	Usando o console ARC	Usando a API ARC
Obter recursos gerenciados	Consulte Recursos compatíveis	Consulte GetManagedResource
Cancelar uma mudança de zona	Consulte Atualizar ou cancelar uma mudança de zona	Consulte CancelZonalShift

Exemplos de uso do AWS CLI com mudança zonal

Esta seção fornece exemplos de aplicação do uso de mudança zonal, usando o AWS Command Line Interface para trabalhar com o recurso de mudança zonal no Amazon Application Recovery Controller (ARC) usando operações de API. Os exemplos têm como objetivo ajudá-lo a desenvolver uma compreensão básica de como trabalhar com a mudança zonal usando a CLI.

A mudança zonal no ARC permite que você mova temporariamente o tráfego dos recursos suportados 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

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 mais informações sobre como usar o AWS CLI, consulte a Referência de AWS CLI Comandos. 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

É possível 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:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05 \
       --away-from use1-az1 \
       --expires-in 10m \
       --comment "Shifting traffic away from use1-az1"
```

```
{
```

```
    "awayFrom": "use1-az1",
    "comment": "Shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T21:37:26-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Obter recursos 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:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05
```

```
{
    "appliedWeights": {
        "use1-az1": 0.0,
        "use1-az2": 1.0,
        "use1-az6": 1.0
    },
    "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/app/
Testing/5a19403ecd42dc05",
    "autoshifts": [],
    "name": "Testing",
    "zonalAutoshiftStatus": "DISABLED",
    "zonalShifts": [
        {
            "appliedStatus": "APPLIED",
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
            "shiftType": "MANUAL"
        }
```

```
    ]
}
```

Listar recursos 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": [
        {
            "appliedWeights": {
                "use1-az1": 0.0,
                "use1-az2": 1.0,
                "use1-az6": 1.0
            },
            "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/
app/Testing/5a19403ecd42dc05",
            "autoshifts": [],
            "availabilityZones": [
                "use1-az1",
                "use1-az2",
                "use1-az6"
            ],
            "name": "Testing",
            "practiceRunStatus": "DISABLED",
            "zonalAutoshiftStatus": "DISABLED",
            "zonalShifts": [
                {
                    "appliedStatus": "APPLIED",
                    "awayFrom": "use1-az1",
                    "comment": "Shifting traffic away from use1-az1",
                    "expiryTime": "2024-12-17T21:37:26-08:00",
                    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
                    "startTime": "2024-12-17T21:27:26-08:00",
                    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
                }
            ]
        }
```

```
    ]
}
```

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": [
        {
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "status": "ACTIVE",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
        }
    ]
}
```

Atualizar mudança de zona

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

```
aws arc-zonal-shift update-zonal-shift \
       --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38 \
       --expires-in 1h \
       --comment "Still shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
```

```
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

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 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Recursos compatíveis

Atualmente, o Amazon Application Recovery Controller (ARC) oferece suporte à habilitação dos seguintes recursos para mudança zonal e mudança automática zonal:

- Grupos do Amazon EC2 Auto Scaling
- Amazon Elastic Kubernetes Service
- Application Load Balancerscom o balanceamento de carga entre zonas ativado ou desativado
- Network Load Balancerscom o balanceamento de carga entre zonas ativado ou desativado

Para requisitos específicos para balanceadores de carga de rede e balanceadores de carga de aplicativos, consulte os tópicos adicionais nesta seção.

Analise as seguintes condições para trabalhar com turnos zonais, deslocamento automático zonal e recursos no ARC:

- 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 um recurso gerenciado no ARC. Por exemplo, visualize a lista de recursos gerenciados no AWS Management Console ou use a `get-managed-resource` operação com o identificador do recurso.
- Para iniciar uma mudança zonal com um recurso, ele deve ser implantado na Zona de Disponibilidade e Região da AWS onde você inicia a mudança. Certifique-se de iniciar uma mudança de zona na mesma região em que a AZ da qual você deseja se afastar está e de que o recurso para o qual você está transferindo o tráfego também esteja na mesma AZ e região.
- Certifique-se de ter as permissões corretas do IAM para usar a mudança de zona com um recurso. Para obter mais informações, consulte IAM e permissões para mudança de zona.
- Quando um Network Load Balancer ou Application Load Balancer está em uma falha, a mudança de zona de estado aberto não terá efeito. Esse é o comportamento esperado porque a mudança de zona não pode forçar uma AZ a ficar insalubre e, em seguida, transferir o tráfego para outra AZs em uma região quando o balanceador de carga está falhando na abertura. Para obter mais informações, consulte Usando o failover de DNS do Route 53 para seu balanceador de carga no Guia do usuário do Network Load Balancers e Usando o failover de DNS do Route 53 para seu balanceador de carga no Guia do usuário do Application Load Balancers.
- Se vários balanceadores de carga estiverem encaminhando tráfego para os mesmos destinos, uma mudança de zona em um balanceador de carga habilitado para várias zonas reduzirá a capacidade alvo de todos os balanceadores de carga, mesmo que eles não sejam deslocados por zona.

Grupos do Amazon EC2 Auto Scaling

Um grupo do Amazon EC2 Auto Scaling contém uma coleção de EC2 instâncias da Amazon que são tratadas como um agrupamento lógico para fins de escalabilidade e gerenciamento automáticos. Um grupo do Auto Scaling também permite que você use os recursos do Amazon Auto EC2 Scaling, como substituições de exames de saúde e políticas de escalabilidade. Tanto a manutenção do número de instâncias em um grupo de Auto Scaling quanto a escalabilidade automática são as principais funcionalidades do serviço Amazon Auto Scaling. EC2

Usando o deslocamento zonal para grupos de Auto Scaling

Para ativar o deslocamento zonal, use um dos métodos a seguir.

Console

Para habilitar a mudança zonal em um novo grupo (console)

1. Siga as instruções em Criar um grupo de Auto Scaling usando um modelo de lançamento e conclua cada etapa do procedimento, até a etapa 10.
2. Na página Integrar com outros serviços, para o deslocamento zonal ARC, marque a caixa de seleção para ativar o deslocamento zonal.
3. Em Comportamento de verificação de integridade, escolha Ignorar não íntegro ou Substituir não íntegro. Se definido como`replace-unhealthy`, as instâncias não íntegras serão substituídas na Zona de Disponibilidade pela mudança de zona ativa. Se definido como`ignore-unhealthy`, as instâncias não íntegras não serão substituídas na Zona de Disponibilidade pela mudança de zona ativa.
4. Continue com as etapas em Criar um grupo de Auto Scaling usando um modelo de lançamento.

AWS CLI

Para habilitar a mudança zonal em um novo grupo ()AWS CLI

Adicione o parâmetro `--availability-zone-impairment-policy` ao comando create-auto-scaling-group.

O `--availability-zone-impairment-policy` parâmetro tem duas opções:

- ZonalShiftEnabled— Se definido como`true`, o Auto Scaling registra o grupo Auto Scaling com o deslocamento zonal ARC e você pode iniciar, atualizar ou cancelar um deslocamento zonal no console ARC. Se definido como`false`, o Auto Scaling cancela o registro do grupo Auto Scaling do deslocamento zonal ARC. Você já deve ter a mudança de zona ativada para `false` definir como.
- ImpairedZoneHealthCheckBehavior— Se definido como`replace-unhealthy`, as instâncias não íntegras serão substituídas na Zona de Disponibilidade pela mudança de zona ativa. Se definido como`ignore-unhealthy`, as instâncias não íntegras não serão substituídas na Zona de Disponibilidade pela mudança de zona ativa.

O exemplo a seguir permite a mudança de zona em um novo grupo de Auto Scaling chamado. *my-asg*

```
aws autoscaling create-auto-scaling-group \
  --launch-template LaunchTemplateName=my-launch-template,Version='1' \
  --auto-scaling-group-name my-asg \
  --min-size 1 \
  --max-size 10 \
  --desired-capacity 5 \
  --availability-zones us-east-1a us-east-1b us-east-1c \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Console

Para habilitar a mudança zonal em um grupo existente (console)

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/e escolha Auto Scaling Groups no painel de navegação.
2. Na barra de navegação na parte superior da tela, escolha a mesma Região da AWS na qual você criou o grupo do Auto Scaling.
3. Marque a caixa de seleção ao lado do grupo do Auto Scaling.

   Um painel dividido é aberto na parte inferior da página.
4. Na guia Integrações, em Deslocamento zonal ARC, escolha Editar.
5. Marque a caixa de seleção para ativar a mudança de zona.
6. Em Comportamento de verificação de integridade, escolha Ignorar não íntegro ou Substituir não íntegro. Se definido como`replace-unhealthy`, as instâncias não íntegras serão substituídas na Zona de Disponibilidade pela mudança de zona ativa. Se definido como`ignore-unhealthy`, as instâncias não íntegras não serão substituídas na Zona de Disponibilidade pela mudança de zona ativa.
7. Selecione Atualizar.

AWS CLI

Para habilitar a mudança zonal em um grupo existente ()AWS CLI

Adicione o parâmetro `--availability-zone-impairment-policy` ao comando update-auto-scaling-group.

O `--availability-zone-impairment-policy` parâmetro tem duas opções:

- ZonalShiftEnabled— Se definido como`true`, o Auto Scaling registra o grupo Auto Scaling com o deslocamento zonal ARC e você pode iniciar, atualizar ou cancelar um deslocamento zonal no console ARC. Se definido como`false`, o Auto Scaling cancela o registro do grupo Auto Scaling do deslocamento zonal ARC. Você já deve ter a mudança de zona ativada para `false` definir como.
- ImpairedZoneHealthCheckBehavior— Se definido como`replace-unhealthy`, as instâncias não íntegras serão substituídas na Zona de Disponibilidade pela mudança de zona ativa. Se definido como`ignore-unhealthy`, as instâncias não íntegras não serão substituídas na Zona de Disponibilidade pela mudança de zona ativa.

O exemplo a seguir permite a mudança de zona no grupo de Auto Scaling especificado.

```
aws autoscaling update-auto-scaling-group --auto-scaling-group-name my-asg \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Para acionar uma mudança de zona, consulte Iniciando, atualizando ou cancelando uma mudança de zona.

Como a mudança zonal funciona para grupos de Auto Scaling

Suponha que você tenha um grupo de Auto Scaling com as seguintes zonas de disponibilidade:

- `us-east-1a`
- `us-east-1b`
- `us-east-1c`

Você percebe falhas `us-east-1a` e aciona uma mudança de zona. Os comportamentos a seguir ocorrem quando uma mudança zonal é acionada`us-east-1a`.

- Escalabilidade horizontal — O Auto Scaling lançará todas as novas solicitações de capacidade nas zonas de disponibilidade saudáveis `us-east-1b` (`us-east-1ce`).
- Escalabilidade dinâmica — O Auto Scaling impedirá que as políticas de escalabilidade diminuam a capacidade desejada. O Auto Scaling não impedirá que as políticas de escalabilidade aumentem a capacidade desejada.
- Atualização de instância — O Auto Scaling estenderá o tempo limite para qualquer processo de atualização de instância que esteja atrasado durante uma mudança de zona ativa.

Seleção de comportamento de verificação de integridade da zona de disponibilidade prejudicada	Comportamento de verificação de saúde
Substitua insalubre	As instâncias que parecem insalubres serão substituídas em todas as zonas de disponibilidade (`us-east-1a us-east-1b` , e `us-east-1c`).
Ignore os não saudáveis	As instâncias que parecem insalubres serão substituídas em `us-east-1b` e. `us-east-1c` As instâncias não serão substituídas na zona de disponibilidade pelo deslocamento zonal ativo (`us-east-1a`).

Melhores práticas para usar o deslocamento zonal

Para manter a alta disponibilidade de seus aplicativos ao usar o deslocamento zonal, recomendamos as seguintes melhores práticas.

- Monitore EventBridge as notificações para determinar quando há um evento contínuo de comprometimento da zona de disponibilidade. Para obter mais informações, consulte Automatização do Amazon Auto EC2 Scaling com o Event Bridge.
- Use políticas de escalabilidade com limites apropriados para garantir que você tenha capacidade suficiente para tolerar a perda de uma zona de disponibilidade.

- Defina uma política de manutenção de instâncias com uma porcentagem íntegra mínima de 100. Com essa configuração, o Auto Scaling espera que uma nova instância esteja pronta para uso antes de encerrar uma instância não íntegra.

Para clientes pré-escalados, também recomendamos o seguinte:

- Selecione Ignorar não íntegro como o comportamento de verificação de integridade da zona de disponibilidade comprometida, pois você não precisa substituir a instância não íntegra durante o evento de comprometimento.
- Use o deslocamento automático zonal no ARC para seus grupos de Auto Scaling. O recurso de mudança automática zonal Controlador de Recuperação de Aplicações (ARC) da Amazon permite AWS deslocar o tráfego de um recurso para fora de uma zona de disponibilidade ao AWS detectar uma deficiência em uma zona de disponibilidade. Para obter mais informações, consulte Mudança automática zonal no ARC no Guia do desenvolvedor do Amazon Application Recovery Controller (ARC).

Para clientes com balanceadores de carga desativados em várias zonas, também recomendamos:

- Use balanceado somente para sua distribuição de zona de disponibilidade.
- Se você estiver usando o deslocamento zonal no grupo do Auto Scaling e nos balanceadores de carga, certifique-se de cancelar primeiro o deslocamento zonal no grupo do Auto Scaling. Em seguida, espere até que a capacidade seja balanceada em todas as zonas de disponibilidade antes de cancelar a mudança zonal no balanceador de carga.
- Devido à possibilidade de desequilíbrio de capacidade quando você ativa a mudança de zona e usa um balanceador de carga desativado entre zonas, o Auto Scaling tem uma validação extra. Se você estiver seguindo as melhores práticas, você pode reconhecer essa possibilidade marcando a caixa de seleção no AWS Management Console ou usando o `skip-zonal-shift-validation` sinalizador em`CreateAutoScalingGroup`,`UpdateAutoScalingGroup`, ou`AttachTrafficSources`.

Amazon Elastic Kubernetes Service

O Amazon EKS fornece recursos que permitem que você torne seus aplicativos mais resilientes a eventos como a degradação da saúde ou o comprometimento de uma zona de disponibilidade (AZ). Ao executar suas cargas de trabalho em um cluster Amazon EKS, você pode melhorar ainda

mais a tolerância a falhas e a recuperação de aplicativos do seu ambiente de aplicativos usando o deslocamento zonal ou o deslocamento automático zonal.

Usando a mudança zonal para o Amazon Elastic Kubernetes Service | Amazon Elastic Kubernetes Service

Para habilitar o deslocamento zonal, use um dos métodos a seguir. Para obter mais informações, consulte Habilitar o deslocamento zonal do Amazon EKS para evitar zonas de disponibilidade prejudicadas.

Console

Para habilitar a mudança zonal em um novo cluster Amazon EKS (console)

1. Encontre o nome e a região do cluster Amazon EKS que você deseja registrar no ARC.
2. Abra o console do Amazon EKS em https://console.aws.amazon.com/eks/home#/clusters.
3. Selecione o cluster
4. Na página de informações do cluster, selecione a guia Overview (Visão geral).
5. No título Mudança de zona, selecione o botão Gerenciar.
6. Selecione ativar ou desativar o EKS Zonal Shift.

AWS CLI

Para habilitar a mudança zonal em um novo cluster Amazon EKS ()AWS CLI

- Digite o comando:

```
aws eks create-cluster --name my-eks-cluster --role-
arn my-role-arn-to-create-cluster --resources-vpc-config
 subnetIds=string,string,securityGroupIds=string,string,endpointPublicAccess=boolean,end
 --zonal-shift-config enabled=true
```

Para habilitar a mudança zonal em um cluster Amazon EKS existente ()AWS CLI

- Digite o comando:

```
aws eks update-cluster-config --name my-eks-cluster --zonal-shift-config
 enabled=true
```

Você pode acionar uma mudança zonal para um cluster Amazon EKS ou permitir que isso seja feito por você ativando AWS a mudança automática zonal. Depois que a mudança zonal do cluster Amazon EKS estiver habilitada com o ARC, você poderá acionar uma mudança zonal ou ativar a mudança automática zonal usando o console ARC, a AWS CLI ou a mudança zonal e a mudança automática zonal. APIs

Para obter mais informações sobre como acionar uma mudança de zona, consulte. Iniciando, atualizando ou cancelando uma mudança de zona

Para obter mais informações sobre como habilitar o Amazon EKS com mudança zonal, consulte o tópico Saiba mais sobre o ARC Zonal Shift no Amazon EKS no Guia do usuário do Amazon Elastic Kubernetes Service.

Como a mudança zonal funciona para o Amazon Elastic Kubernetes Service | Amazon Elastic Kubernetes Service

Durante uma mudança de zona do Amazon EKS, o seguinte ocorrerá automaticamente:

- Todos os nós na AZ afetada serão isolados. Isso impedirá que o Kubernetes Scheduler agende novos pods para os nós na AZ não íntegra.
- Se você estiver usando grupos de nós gerenciados, o rebalanceamento da zona de disponibilidade será suspenso e seu grupo de Auto Scaling (ASG) será atualizado para garantir que os novos nós do plano de dados do Amazon EKS sejam lançados somente em bom estado. AZs
- Os nós na AZ não íntegros não serão encerrados, e os pods não serão despejados desses nós. Isso é para garantir que, quando uma mudança de zona expirar ou for cancelada, seu tráfego possa ser devolvido com segurança para a AZ, que ainda tem capacidade total.
- O EndpointSlice controlador encontrará todos os endpoints do Pod na AZ danificada e os removerá da unidade relevante EndpointSlices. Isso garantirá que somente os endpoints do Pod em bom estado AZs sejam direcionados para receber tráfego de rede. Quando uma mudança de zona é cancelada ou expira, o EndpointSlice controlador atualiza o EndpointSlices para incluir os endpoints na AZ restaurada.

Para obter mais informações, consulte o blog AWS Containers.

Application Load Balancers

Usando o deslocamento zonal para balanceadores de carga de aplicativos

Para usar o Application Load Balancers com o deslocamento zonal, você deve habilitar a integração do deslocamento zonal ARC nos atributos do Application Load Balancer. O Application Load Balancer oferece suporte à mudança de zona com configurações ativadas ou desativadas entre zonas.

Antes de habilitar a integração do ARC e começar a utilizar o deslocamento zonal, analise o seguinte:

- Você pode iniciar uma mudança de zona para um balanceador de carga específico somente para uma única zona de disponibilidade. Você não pode iniciar uma mudança de zona para várias zonas de disponibilidade.
- AWS remove proativamente os endereços IP do balanceador de carga zonal do DNS quando vários problemas de infraestrutura afetam os serviços. Antes de iniciar uma mudança de zona, sempre verifique a capacidade atual da zona de disponibilidade.
- Quando um Application Load Balancer for o destino de um Network Load Balancer, sempre inicie a mudança de zona pelo Network Load Balancer. Se você iniciar uma mudança de zona pelo Application Load Balancer, o Network Load Balancer não reconhecerá a mudança e continuará a enviar tráfego para o Application Load Balancer.

Você pode iniciar uma mudança de zona para um balanceador de carga no console do Elastic Load Balancing (na Regiões da AWS maioria) ou no console ARC.

Console

Para habilitar a mudança de zona em um balanceador de carga (console)

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. Na página de navegação, em Balanceamento de carga, escolha Balanceadores de carga.
3. Selecione o nome do Application Load Balancer.
4. Na guia Atributos, escolha Editar.
5. Em Configuração de roteamento da zona de disponibilidade, defina Integração de mudança de zona do ARC como Habilitar.
6. Escolha Salvar.

AWS CLI

Para habilitar a mudança zonal em um balanceador de carga ()AWS CLI

- Digite o comando:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-alb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

Para obter mais informações sobre como acionar uma mudança de zona, consulte. Iniciando, atualizando ou cancelando uma mudança de zona

Você pode usar a `keepalive` opção para configurar por quanto tempo as conexões continuarão. Para obter mais informações, consulte a duração do keepalive do cliente HTTP no Guia do usuário do Application Load Balancer. Por padrão, os Application Load Balancers definem o valor da duração do keepalive do cliente HTTP como 3.600 segundos ou 1 hora. Sugerimos que você reduza o valor para estar alinhado com a meta de tempo de recuperação do aplicativo, por exemplo, 300 segundos. Ao escolher o tempo de duração do keepalive de um cliente HTTP, considere que esse valor é uma troca entre se reconectar com mais frequência em geral, o que pode afetar a latência, e afastar mais rapidamente todos os clientes de uma AZ ou região com problemas.

Como a mudança de zona funciona para balanceadores de carga de aplicativos

Quando uma mudança de zona é iniciada em um Application Load Balancer com o balanceamento de carga entre zonas ativado, todo o tráfego para destinos é bloqueado na zona de disponibilidade afetada e remove o endereço IP zonal do DNS.

Para obter mais informações, consulte Integrações para seu Application Load Balancer no Guia do usuário do Application Load Balancer.

Network Load Balancers

Usando a mudança zonal para balanceadores de carga de rede

Para usar Network Load Balancers com deslocamento zonal, você deve habilitar a integração do deslocamento zonal ARC nos atributos do Network Load Balancer. O Network Load Balancer suporta mudança de zona com configurações habilitadas ou desabilitadas entre zonas.

Você pode escolher quais recursos optar por usar o deslocamento zonal e o deslocamento automático zonal e quando gostaria de sair de uma zona de disponibilidade prejudicada. Há suporte para balanceadores de carga de rede internos e voltados para a Internet.

Para habilitar a mudança de zona para seu Network Load Balancer habilitado para várias zonas, todos os grupos-alvo conectados ao balanceador de carga devem atender aos seguintes requisitos.

- O balanceamento de carga entre zonas deve estar ativado ou definido como. `use_load_balancer_configuration`
  - Para obter mais informações sobre o balanceamento de carga entre zonas do grupo-alvo, consulte Balanceamento de carga entre zonas para grupos-alvo.
- O protocolo do grupo-alvo deve ser TCP ou TLS.
  - Para obter mais informações sobre os protocolos do grupo alvo do Network Load Balancer, consulte Configuração de roteamento.
- O encerramento da conexão para alvos não íntegros deve ser desativado.
  - Para obter mais informações sobre o término da conexão do grupo-alvo, consulte Encerramento da conexão para destinos não íntegros.
- O grupo-alvo não deve ter nenhum Application Load Balancer como destino.
  - Para obter mais informações sobre Application Load Balancers como destinos, consulte Usar Application Load Balancers como destinos de um Network Load Balancer.

Você pode iniciar uma mudança de zona para um Network Load Balancer usando AWS CLI o, o console ou AWS o widget Elastic Load Balancing. Quando um Application Load Balancer é o destino de um Network Load Balancer, você deve iniciar a mudança zonal do Network Load Balancer. Se você iniciar a mudança de zona a partir do Application Load Balancer, o Network Load Balancer não deixará de enviar tráfego para o Application Load Balancer e seus destinos.

Console

Para habilitar a mudança de zona em um balanceador de carga (console)

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. Na página de navegação, em Balanceamento de carga, escolha Balanceadores de carga.
3. Selecione o nome do Network Load Balancer.
4. Na guia Atributos, escolha Editar.

5. Em Configuração de roteamento da zona de disponibilidade, defina Integração de mudança de zona do ARC como Habilitar.
6. Escolha Salvar.

AWS CLI

Para habilitar a mudança zonal em um balanceador de carga ()AWS CLI

- Digite o comando:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-nlb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

Para obter mais informações sobre como acionar uma mudança de zona, consulte. Iniciando, atualizando ou cancelando uma mudança de zona

Como a mudança zonal funciona para balanceadores de carga de rede

O ARC induz uma falha na verificação de integridade do Network Load Balancer registrado, portanto, o nó Network Load Balancer na AZ prejudicada é removido do DNS quando você aciona uma mudança de zona. O Network Load Balancer desativará os alvos na zona afetada para que eles parem de receber tráfego, e o Elastic Load Balancing trata esses alvos como alvos desativados por mudança de zona. Os alvos no estado desativado continuam recebendo exames de saúde. Quando os alvos estão saudáveis e a mudança zonal expira (ou é cancelada), o roteamento para os alvos na zona anteriormente comprometida é retomado.

Durante a mudança de zona nos Network Load Balancers com o balanceamento de carga entre zonas habilitado, os endereços IP do balanceador de carga de zona são removidos do DNS. As conexões existentes com destinos na zona de disponibilidade comprometida persistem até serem fechadas organicamente, enquanto as novas conexões não são mais roteadas para alvos na zona de disponibilidade comprometida.

Para obter mais informações, consulte o tópico Zonal Shift for your Network Load Balancer no Guia do usuário do Network Load Balancer.

Iniciando, atualizando ou cancelando uma mudança de zona

Esta seção fornece procedimentos para trabalhar com turnos zonais, incluindo iniciar um turno zonal e cancelar um turno zonal.

Iniciar uma mudança de zona

As etapas desta seção explicam como iniciar uma mudança de zona iniciada pelo cliente no console do Amazon Application Recovery Controller (ARC). Para trabalhar com a mudança de zona de forma programática, consulte o Guia de referência da API de mudança de zona.

Além de iniciar uma mudança zonal no ARC, você também pode iniciar uma mudança zonal para um balanceador de carga no console do Elastic Load Balancing (nas regiões suportadas). Para obter mais informações, consulte Mudança zonal no Guia do Usuário do Elastic Load Balancing.

Como iniciar uma mudança de zona

1. Abra o console ARC 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 recurso compatível na tabela Recursos para o qual transferir 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 cancela uma mudança de zona no console do Amazon Application Recovery Controller (ARC). 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 os turnos zonais que você inicia ou os turnos zonais que AWS começam para um recurso para uma execução prática de mudança automática zonal. Para saber mais sobre a prática de turnos no deslocamento automático zonal, consulte. Como a mudança automática de zona e as execuções práticas funcionam

Como atualizar uma mudança de zona

1. Abra o console ARC 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. Selecione Atualizar.

Como cancelar uma mudança de zona

1. Abra o console ARC 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.

Registro e monitoramento para mudança de zona no Amazon Application Recovery Controller (ARC)

Você pode usar AWS CloudTrail para monitorar a mudança de zona no Amazon Application Recovery Controller (ARC), para analisar padrões e ajudar a solucionar problemas.

Tópicos

- Registrando chamadas de API de mudança zonal usando AWS CloudTrail

Registrando chamadas de API de mudança zonal usando AWS CloudTrail

A mudança zonal para ARC é integrada com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no ARC. CloudTrail captura todas as chamadas de API para mudança de zona como eventos. As chamadas capturadas incluem chamadas do console ARC e chamadas de código para as operações da API ARC para mudança de zona.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para mudança de zona. 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 ARC para mudança de zona, 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 de mudança zonal em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no ARC para mudança de zona, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos de mudança zonal no 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 eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do ARC são registradas CloudTrail e documentadas no Guia de referência da API Routing Control para o Amazon Application Recovery Controller. Por exemplo, chamadas para as `ListManagedResources` ações `StartZonalShift` e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Visualizando eventos ARC no histórico de eventos

CloudTrail permite que você visualize eventos recentes no histórico de eventos. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário.

Compreendendo as entradas do arquivo de log de mudança zonal

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 `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"
      }
    }
```

Identity and Access Management para mudança de zona no Amazon Application Recovery Controller (ARC)

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 (conectado) e autorizado (tem permissões) para usar os recursos do ARC. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Conteúdo

Como a mudança zonal funciona com o IAM

Antes de usar o IAM para gerenciar o acesso à mudança zonal no Amazon Application Recovery Controller (ARC), saiba quais recursos do IAM estão disponíveis para uso com a mudança zonal.

Recursos do IAM que você pode usar com a mudança zonal

Atributo do IAM	Suporte de mudança zonal
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não

Atributo do IAM	Suporte de mudança zonal
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para obter uma visão geral de alto nível de como os AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS Serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para ARC

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 do IAM, grupo de usuários ou perfil. 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 Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim 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 perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Para ver exemplos de políticas baseadas em identidade do ARC, consulte. Exemplos de políticas baseadas em identidade no Amazon Application Recovery Controller (ARC)

Políticas baseadas em recursos dentro do ARC

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos 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 políticas para mudança zonal

Compatível com 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 podem ser usadas 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. Algumas operações também 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 de ações do ARC para mudança de zona, consulte Ações definidas pelo Amazon Route 53 Zonal Shift na Referência de Autorização de Serviço.

As ações políticas no ARC para mudança zonal usam os seguintes prefixos antes da ação:

```
arc-zonal-shift
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas. Por exemplo, o seguinte:

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift: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": "arc-zonal-shift:Describe*"
```

Para ver exemplos de políticas baseadas em identidade do ARC para mudança de zona, consulte. Exemplos de políticas baseadas em identidade para mudança zonal no ARC

Recursos políticos para mudança zonal

Compatível com 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 de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um 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 você pode especificar com o ARN de cada recurso, consulte o tópico a seguir na Referência de Autorização de Serviço:

- Ações definidas pelo Amazon Route 53 - Zonal Shift

Para ver as ações e os recursos que você pode usar com uma chave de condição, consulte o tópico a seguir na Referência de Autorização de Serviço:

- Chaves de condição definidas pelo Amazon Route 53 - Zonal Shift

Para ver exemplos de políticas baseadas em identidade do ARC para mudança de zona, consulte. Exemplos de políticas baseadas em identidade para mudança zonal no ARC

Chaves de condição de política para mudança zonal

Compatível com chaves de condição de política específicas de 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 `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões

condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `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 antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar 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 da 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 das chaves de condição de mudança zonal, consulte o tópico a seguir na Referência de Autorização de Serviço:

- Chaves de condição definidas pelo Amazon Route 53 - Zonal Shift

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 Amazon Route 53 - Zonal Shift
- Tipos de recursos definidos pelo Amazon Route 53 - Zonal Shift

Para ver exemplos de políticas baseadas em identidade do ARC para mudança de zona, consulte. Exemplos de políticas baseadas em identidade para mudança zonal no ARC

Listas de controle de acesso (ACLs) em ARC

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso baseado em atributos (ABAC) com ARC

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as 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. Marcar de entidades e atributos 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 estiver 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 chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do 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 ARC inclui o seguinte suporte parcial para ABAC:

- O deslocamento zonal suporta o ABAC para recursos gerenciados que são registrados no ARC para o deslocamento zonal. 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.

Usando credenciais temporárias com o ARC

Compatível com 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 “Trabalhe 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 funções, consulte Alternar para um perfil do IAM (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 principais entre serviços para ARC

Compatibilidade com o recurso de 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. Permissões concedidas por políticas a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, acionar outra ação em outro serviço. Nesse caso, você precisa ter permissões para executar ambas as ações.

Para ver se uma ação exige ações dependentes adicionais em uma política, consulte o tópico a seguir na Referência de Autorização de Serviço:

- Mudança de zona do Amazon Route 53

Funções de serviço para ARC

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar 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.

Funções vinculadas a serviços para ARC

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções

vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

A mudança de zona não usa funções vinculadas a serviços.

IAM e permissões para mudança de zona

Esta seção fornece informações adicionais sobre como as permissões funcionam para o recurso de mudança de zona no Amazon Application Recovery Controller (ARC), especialmente se você trabalha com o recurso de outro AWS serviço, como o Elastic Load Balancing. Para saber como os recursos do ARC funcionam com o IAM e as permissões em geral, revise as informações no tópico de visão geral,Identity and Access Management para mudança de zona no Amazon Application Recovery Controller (ARC).

A mudança zonal é compatível com balanceadores de carga de aplicativos, balanceadores de carga de rede, grupos do Amazon EC2 Auto Scaling e Amazon EKS. Você pode usar as chaves de condição do IAM para definir o escopo de uma política de permissão do IAM para esses recursos. Veja a seguir um exemplo de política usando uma chave de condição com vários recursos de diferentes tipos:

```
{
    "Condition": {
        "StringLike": {
            "arc-zonal-shift:ResourceIdentifier": [
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/
*",
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/
*",
                "arn:aws:eks:us-east-1:123456789012:cluster/*"
            ]
        }
    },
    "Action": [
        "arc-zonal-shift:StartZonalShift"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
```

Para obter mais informações, consulte Recursos compatíveis.

Além das permissões descritas no tópico de visão geral do IAM, o seguinte se aplica à mudança de zona para IAM e permissões:

- Certifique-se de ter as permissões necessárias para trabalhar com a mudança zonal no ARC. Para obter mais informações, consulte acesso ao console de mudança zonal e acesso às operações de mudança zonal.
- Você não precisa adicionar permissões adicionais do Elastic Load Balancing com o IAM para trabalhar com mudanças zonais para recursos gerenciados de balanceador de carga em sua conta no 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 para mudança zonal no ARC

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do ARC. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos 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 aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo ARC, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon Application Recovery Controller (ARC) na Referência de autorização de serviço. ARNs

Tópicos

- Práticas recomendadas de política
- Exemplo: acesso ao console de mudança zonal
- Exemplo: ações da API de mudança zonal

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos ARC em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance 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 funções 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 da 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 cem verificações de política e recomendações práticas para ajudar 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 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 de mudança zonal

Para acessar o console do Amazon Application Recovery Controller (ARC), você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do ARC em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva 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 à operação de API que estiverem tentando executar.

Para dar aos usuários acesso total ao uso da mudança de zona no AWS Management Console, 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": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

Exemplo: ações da API de mudança zonal

A API de mudança zonal retira temporariamente o tráfego de uma zona de disponibilidade para recuperar um aplicativo.

Para garantir que um usuário possa usar ações de API de mudança de zona, anexe uma política que corresponda às operações de API com as quais o usuário precisa trabalhar, como a seguinte:

```
{
    "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": "*"
        }
    ]
}
```

Mudança automática zonal em ARC

Com o deslocamento automático zonal, você AWS autoriza a transferência do tráfego de recursos de um aplicativo de uma zona de disponibilidade (AZ) durante eventos, em seu nome, para ajudar a reduzir o tempo de recuperação. AWS inicia um deslocamento automático quando a telemetria interna indica que há uma deficiência na zona de disponibilidade que pode afetar potencialmente os clientes. Quando AWS inicia um deslocamento automático, o tráfego do aplicativo para os recursos que você configurou para o deslocamento automático zonal começa a se afastar da Zona de Disponibilidade.

Esteja ciente de que o ARC não inspeciona a integridade dos recursos individuais. AWS inicia um deslocamento automático quando a AWS telemetria detecta que há uma deficiência na zona de disponibilidade que poderia afetar potencialmente os clientes. Em alguns casos, o tráfego pode ser desviado para recursos que não estão sofrendo impacto.

Com o deslocamento automático zonal, você também AWS autoriza a transferência do tráfego de recursos de um aplicativo 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 zonais que o ARC inicia para execução prática ajudam você a garantir que o deslocamento do tráfego de uma zona de disponibilidade durante um deslocamento automático seja seguro para seu aplicativo. 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 o aplicativo funciona conforme o esperado.

> **Important**
>
> Antes de configurar as execuções práticas ou ativar o deslocamento automático zonal, é altamente recomendável que você pré-escale a capacidade dos recursos do aplicativo em todas as zonas de disponibilidade na região em que os recursos do aplicativo 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. Confiar no escalonamento automático, em vez do pré-escalonamento, pode fazer com que o aplicativo demore mais para se recuperar.
> 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 ativar o deslocamento automático zonal ou configurar execuções práticas, depois de pré-dimensionar a capacidade de recursos do aplicativo, teste se o aplicativo pode 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 habilitar o deslocamento automático zonal, recomendamos que você verifique, iniciando e avaliando uma mudança zonal de execução prática sob demanda, se seu aplicativo pode continuar operando normalmente com o tráfego deslocado para fora de uma zona de disponibilidade.
Em seguida, as execuções práticas regulares que o ARC realiza ajudam você a confirmar, continuamente, que você tem capacidade suficiente para um deslocamento automático.

Para garantir que seus testes com mudança de zona sejam eficazes, é importante validar se o tráfego é drenado conforme o esperado da AZ da qual você se afasta. Por exemplo, tanto os Application Load Balancers quanto os Network Load Balancers fornecem métricas por AZ na Amazon CloudWatch que você pode usar para monitorar isso. Dependendo de quanto tempo um serviço e os clientes reutilizam as conexões, o tráfego pode continuar para a AZ da qual você se afastou por mais tempo do que o esperado. Para saber mais, consulte Limitar o tempo que os clientes permanecem conectados aos seus endpoints.

Você pode ativar o deslocamento automático zonal, para um recurso compatível, no console ARC. Ou, no EC2 console da Amazon, você tem a opção de ativar o deslocamento automático zonal para um recurso específico de balanceador de carga. Para saber mais sobre como habilitar o deslocamento automático zonal com o Elastic Load Balancing, consulte Mudança zonal no Guia do Usuário do Elastic Load Balancing.

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, AWS deixa de transferir o tráfego de 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 obter mais informações, consulte Usando o deslocamento automático zonal com a Amazon EventBridge.

Como a mudança automática de zona e as execuções práticas funcionam

A capacidade de mudança automática zonal no Amazon Application Recovery Controller (ARC) permite AWS transferir o tráfego de um recurso para fora de uma zona de disponibilidade, em seu nome, quando AWS determina que há uma deficiência que poderia afetar os clientes na zona de disponibilidade. O deslocamento automático zonal foi projetado para um recurso pré-escalado em todas as zonas de disponibilidade em um Região da AWS, para que um aplicativo possa operar normalmente com a perda de uma zona de disponibilidade.

Com o deslocamento automático zonal, você precisa configurar execuções práticas, nas quais o ARC regularmente transfere o tráfego do recurso para fora de uma zona de disponibilidade. O ARC agenda execuções práticas aproximadamente semanalmente para cada recurso que tem uma configuração de execução prática associada a ele. As execuções práticas são agendadas de forma independente para cada recurso.

Para cada treino, o 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 obter mais informações, consulte Usando o deslocamento automático zonal com a Amazon EventBridge.

Conteúdo

Sobre o deslocamento automático 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 deve ativar manualmente o deslocamento automático zonal para os recursos compatíveis AWS .

Quando você implanta e executa AWS aplicativos em balanceadores de carga em vários (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 reduzindo o

tráfego com um deslocamento automático. Ao transferir o tráfego de recursos para outros AZs na região, AWS pode 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.

Os recursos suportados pelo ARC fornecem integrações que marcam a AZ especificada como não íntegra, o que resulta no afastamento do tráfego da AZ prejudicada.

Ao habilitar o deslocamento automático zonal para um recurso, você também deve configurar uma execução prática para o recurso. AWS realiza execuções práticas cerca de uma vez por semana, por 30 minutos, para ajudá-lo a garantir que você tenha capacidade suficiente para executar seu aplicativo sem uma das zonas de disponibilidade na 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-alvo do balanceador de carga no AZs não tiverem nenhuma instância ou se todas as instâncias não estiverem íntegras, o balanceador de carga estará em um estado de falha aberta e você não poderá transferir uma delas. AZs

Para saber mais sobre a mudança automática de zona, consulte Mudança automática zonal em ARC.

Quando AWS inicia e para as mudanças automáticas

Ao habilitar o deslocamento automático zonal para um recurso, você AWS autoriza a transferência do tráfego de recursos de um aplicativo de uma zona de disponibilidade durante eventos, em seu nome, para ajudar a reduzir o tempo de recuperação.

Para conseguir isso, o deslocamento automático zonal usa a AWS telemetria para detectar, o mais cedo possível, que há uma deficiência na zona de disponibilidade que poderia 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.

O deslocamento automático zonal é um recurso projetado para clientes que pré-escalaram seus recursos de aplicativos para todas as zonas de disponibilidade em um. Região da AWS Você não deve depender da escalabilidade sob demanda quando uma mudança automática ou um treino começa.

AWS encerra um deslocamento automático quando determina que a zona de disponibilidade foi recuperada.

Quando o ARC agenda, inicia e termina, os treinos correm

O ARC agenda uma execução prática para um recurso semanalmente, por cerca de 30 minutos. O ARC agenda, inicia e gerencia execuções práticas para cada recurso de forma independente. O ARC não agrupa execuções práticas para recursos na mesma conta. Você também pode iniciar exercícios sob demanda para ajudar a verificar se sua configuração é segura para um evento de mudança automática zonal.

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 ARC interrompe uma execução prática e a encerra. Por exemplo, se um turno automático começar durante uma corrida de treino, o ARC interrompe a corrida de treino e a encerra. 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 ARC também interrompe a execução da prática e a encerra.

Além disso, há vários cenários em que o ARC não inicia uma execução prática de agendamento para um recurso.

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

- Se a execução prática de um recurso for interrompida enquanto estiver em andamento, o ARC considera que a execução prática semanal terminou e agenda uma nova execução prática do recurso para a próxima semana. 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 ARC não iniciará a execução prática. O ARC continua monitorando regularmente, para determinar se ainda há uma ou mais restrições de bloqueio. Quando não há nenhuma restrição de bloqueio, o ARC inicia a execução prática do recurso.

A seguir estão exemplos de restrições de bloqueio que impedem o ARC de iniciar ou continuar uma execução prática para um recurso:

- O ARC não inicia nem continua os treinos quando há um AWS Fault Injection Service experimento em andamento. Se um AWS FIS evento estiver ativo quando o ARC tiver agendado o início de uma corrida prática, o ARC não iniciará a corrida prática. O ARC monitora durante todo o treino as restrições de bloqueio, incluindo um AWS FIS evento. Se um AWS FIS evento começar enquanto um treino estiver ativo, o ARC encerrará o treino e não tentará iniciar outro até a próxima corrida de treinos regularmente agendada para o recurso.
- Se houver um AWS evento atual em uma região, o ARC não inicia os treinos para obter recursos e encerra os treinos ativos na região.

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

Verificações de capacidade para treinos

Quando uma execução prática começa, para afastar temporariamente o tráfego de uma zona de disponibilidade, o ARC executa uma verificação para verificar se você tem capacidade suficiente em outras zonas de disponibilidade para afastar o tráfego com segurança da AZ. Se não houver capacidade suficiente disponível, a mudança de tráfego para a corrida prática não será iniciada e a corrida prática será encerrada.

Além disso, o ARC executa uma verificação de capacidade dos recursos do balanceador de carga quando um deslocamento automático zonal é concluído, antes que o ARC encerre o deslocamento de tráfego iniciado pelo deslocamento automático. Se a verificação de capacidade falhar quando o deslocamento automático terminar, o tráfego não será transferido de volta para a zona de disponibilidade da qual foi retirado.

As verificações de capacidade balanceada só são concluídas para balanceadores de carga e grupos de Auto Scaling.

Para um recurso de balanceador de carga, as verificações de capacidade validam se os hosts saudáveis associados ao balanceador de carga estão distribuídos entre as zonas de disponibilidade. Especificamente, as verificações de capacidade garantem que o número de hosts saudáveis

em todas as zonas de disponibilidade em que o recurso está registrado seja balanceado. Para verificações de capacidade, balanceada significa que a capacidade íntegra de cada zona de disponibilidade está em paridade com as outras zonas, dentro de uma pequena variação.

Observe que as verificações de capacidade não são aplicadas a balanceadores de carga com grupos-alvo do tipo Lambda nem a balanceadores de carga de aplicativos, porque esses destinos não são configurados zonalmente.

As verificações de capacidade também são concluídas para grupos de Auto Scaling. Para um grupo de Auto Scaling, as verificações de capacidade validam que a capacidade zonal total íntegra de um grupo de Auto Scaling, ou seja, o número total de hosts íntegros em todas as zonas de disponibilidade, atende ao conjunto de capacidades desejado para esse grupo de Auto Scaling.

Quando uma verificação de capacidade falha

Quando uma verificação de capacidade descobre que a capacidade disponível não está balanceada para um recurso, o resultado da execução prática é`CAPACITY_CHECK_FAILED`. Para saber mais sobre por que uma verificação de capacidade falhou, consulte o campo de comentários do`ZonalShiftSummary`. Para encontrar o campo de comentários para sua prática, execute zonal shift, faça o seguinte:

1. Usando o AWS CLI, liste as mudanças de zona para o recurso que você especificou na execução prática usando a operação da ListZonalShiftsAPI.

   FOr exemplo, para retornar as mudanças zonais, você pode executar um comando semelhante ao seguinte:

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

2. Examine a matriz de `ZonalShiftSummary` objetos retornados para encontrar a mudança de zona da execução prática que falhou devido às verificações de capacidade.
3. Para o deslocamento zonal aplicável, revise as informações no `Comment` campo.

Notificação para treinos e turnos automáticos

Você pode optar por ser notificado sobre ensaios e mudanças automáticas para seu recurso configurando as notificações da Amazon EventBridge . Você pode configurar EventBridge notificações mesmo quando não tiver ativado o deslocamento automático zonal para nenhum

recurso, conhecido como notificação do observador de mudança automática. Com a notificação do observador de mudança automática, você é notificado sobre todas as mudanças automáticas que o ARC inicia quando uma zona de disponibilidade está potencialmente comprometida. Observe que você deve configurar essa opção em cada uma Região da AWS das quais deseja receber notificações.

Para ver as etapas para habilitar a notificação do observador de mudança automática, consulte. Ativando ou desativando a notificação do observador de deslocamento automático Para saber mais sobre as opções de notificação e como configurá-las EventBridge, consulteUsando o deslocamento automático zonal com a Amazon EventBridge.

Precedência para mudanças zonais

Não pode haver mais do que um deslocamento zonal aplicado em um determinado momento. Ou seja, apenas uma prática executa mudança zonal, mudança zonal iniciada pelo cliente, mudança automática ou AWS FIS experimento para o recurso. Quando uma segunda mudança zonal é iniciada, o ARC segue uma precedência para determinar qual tipo de mudança zonal está em vigor para um recurso.

O princípio geral de precedência é que os turnos zonais que você inicia como cliente têm precedência sobre outros tipos de turno. No entanto, esteja ciente de que uma execução prática AWS iniciada atualmente impede que você inicie uma execução prática sob demanda.

Para ilustrar a precedência no ARC, veja a seguir como a precedência funciona em cenários de exemplo:

Tipo de deslocamento zonal aplicado	Tipo de mudança zonal iniciado	Resultado
AWS FIS experimento	Corrida de treino	A execução prática não será iniciada, pois o AWS FIS experimento tem precedência.
AWS FIS experimento	Mudança zonal manual	O AWS FIS experimento será cancelado e a mudança de zona manual será aplicada.
AWS FIS experimento	Mudança automática de zona	O AWS FIS experimento será cancelado e o deslocame

Tipo de deslocamento zonal aplicado	Tipo de mudança zonal iniciado	Resultado
		nto automático zonal será aplicado.
AWS FIS experimento	AWS FIS experimento	O AWS FIS experimento iniciado não será iniciado porque há um experimento em execução que acionou a ação de AWS FIS mudança automática.
Corrida de treino	Mudança zonal manual	A corrida de treinos será cancelada e o resultado definido como`INTERRUPTED`, e a mudança zonal será aplicada.
Corrida de treino	AWS FIS experimento	A corrida prática será cancelada e o resultado definido`INTERRUPTED`, e o AWS FIS experimento será aplicado.
Corrida de treino	Mudança automática de zona	A execução prática será cancelada e o resultado definido como`INTERRUPTED`, e a mudança automática zonal será aplicada.
Mudança zonal manual	Corrida de treino	A corrida prática não começará.
Mudança zonal manual	AWS FIS experimento	O AWS FIS experimento não será iniciado ou falhará se já estiver em andamento.

Tipo de deslocamento zonal aplicado	Tipo de mudança zonal iniciado	Resultado
Mudança zonal manual	Mudança automática de zona	O deslocamento automático zonal será `ACTIVE`, mas não `APPLIED` no recurso. A mudança zonal manual tem precedência.
Mudança automática de zona	AWS FIS experimento	O AWS FIS experimento não começará ou falhará se estiver em andamento.
Mudança automática de zona	Mudança zonal manual	O deslocamento automático zonal será `ACTIVE`, mas não `APPLIED` no recurso. A mudança zonal manual tem precedência.
Mudança automática de zona	Corrida de treino	A execução prática não será iniciada, pois o deslocamento automático zonal tem precedência.

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. Outros turnos que estão em andamento estão definidos como`NOT_APPLIED`, mas permanecem com `ACTIVE` status.

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

Para interromper um deslocamento automático em andamento para um recurso, você deve cancelar o deslocamento zonal.

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, AWS interrompe a execução de execuções práticas que afastam o tráfego do recurso de uma zona de disponibilidade a cada semana. Além disso, como o deslocamento automático zonal requer execuções práticas, quando você exclui uma configuração de execução prática usando o console ARC, essa ação também desativa o deslocamento automático zonal 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 obter mais informações, consulte Cancelamento de um deslocamento automático zonal e Habilitando e trabalhando com o deslocamento automático zonal.

Como o tráfego é transferido

Para turnos automáticos e para turnos zonais de execução prática, o tráfego é retirado de uma zona de disponibilidade usando o mesmo mecanismo que o ARC usa para turnos zonais iniciados pelo cliente. Uma verificação de integridade não íntegra faz com que o Amazon Route 53 retire os endereços IP correspondentes do recurso do DNS, para que o tráfego seja redirecionado da zona de disponibilidade. Em vez Região da AWS disso, novas conexões são roteadas para outras zonas de disponibilidade.

Com um deslocamento automático, quando uma zona de disponibilidade se recupera e AWS decide encerrar o deslocamento automático, o ARC reverte o processo de verificação de saúde, solicitando que as verificações de saúde do Route 53 sejam revertidas. Em seguida, os endereços IP zonais originais são restaurados e, se as verificações de integridade continuarem íntegras, a Zona de Disponibilidade será incluída novamente no roteamento do aplicativo.

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 ARC usa verificações de saúde para afastar o tráfego das zonas de disponibilidade, solicitando que as verificações de saúde sejam definidas como não íntegras e, em seguida, restaura as verificações de saúde ao normal novamente ao encerrar um deslocamento automático ou uma mudança zonal.

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 Práticas recomendadas ao configurar o deslocamento automático zonal.

O alarme de resultado também fornece informações sobre o resultado do treino que o ARC relata para cada execução do treino. 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 agendado 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 os treinos 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 agendada 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`.

Região da AWS disponibilidade para mudança automática zonal

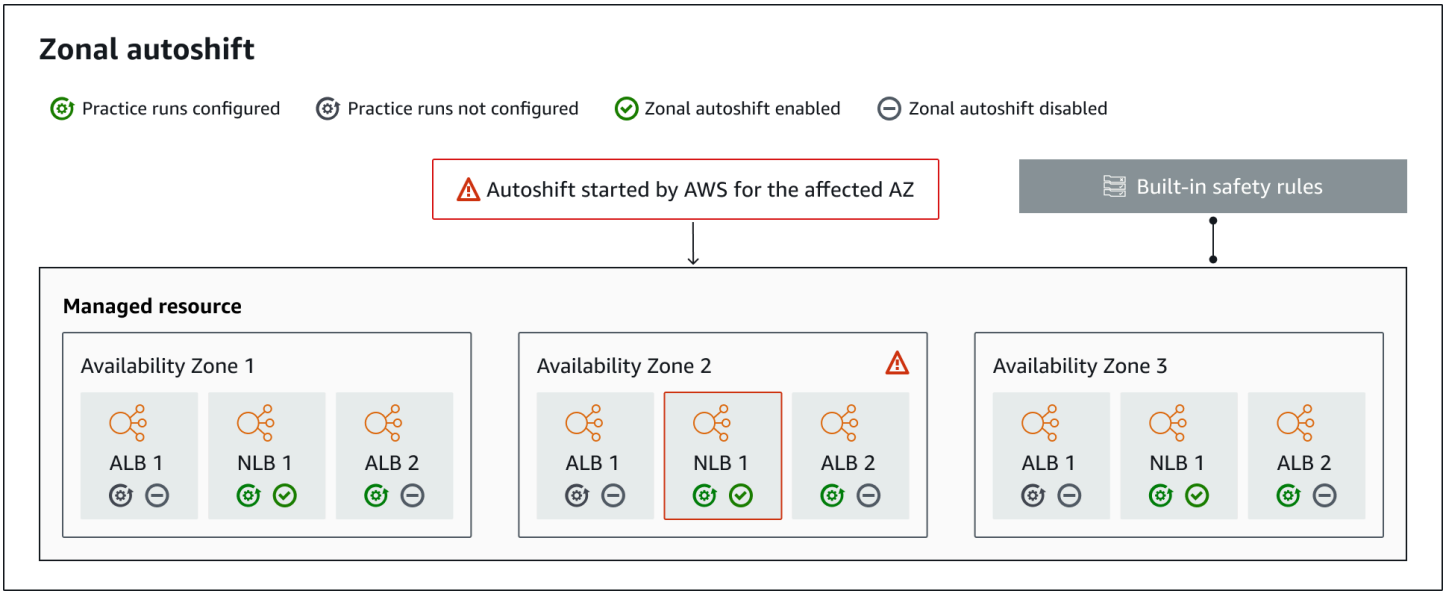
Atualmente, o deslocamento zonal e o deslocamento automático zonal estão disponíveis nas regiões comercial Regiões da AWS, bem como nas regiões da China, ou seja, na região da China (Pequim) e na região da China (Ningxia).

Os recursos que usam o Amazon Application Recovery Controller (ARC) podem incluir considerações adicionais. Para obter mais informações, consulte Recursos compatíveis.

Para obter uma lista de regiões e informações detalhadas sobre endpoints regionais de suporte e serviço para ARC, consulte os endpoints e cotas do Amazon Application Recovery Controller (ARC) na Referência geral da Amazon Web Services.

Componentes da mudança automática de zona

O diagrama a seguir ilustra um exemplo de um deslocamento automático retirando o tráfego de uma zona de disponibilidade. 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 seguir estão os componentes dos recursos de mudança automática zonal no 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 ARC que AWS inicia um deslocamento automático quando a telemetria interna indica que há uma deficiência na zona de disponibilidade que pode afetar potencialmente 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. Você também pode programar sessões de treino sob demanda.

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 uma execução AWS prática para um recurso no deslocamento automático zonal. Você pode editar uma configuração de execução prática a qualquer momento, para adicionar ou alterar datas ou janelas bloqueadas, ou para atualizar os alarmes da execução prática.

Para habilitar o deslocamento automático zonal, você deve ter uma configuração de execução prática em vigor 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 `ALARM` estado, o ARC encerrará a mudança de zona para a execução da prática, de forma que o tráfego do recurso não seja mais desviado 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

O ARC relata um resultado para cada treino. 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.
- CAPACITY_CHECK_FAILED: A verificação da capacidade balanceada entre as zonas de disponibilidade dos recursos do grupo de balanceamento de carga e Auto Scaling falhou.

Regras de segurança integradas

As regras de segurança incorporadas ao ARC evitam que mais de uma mudança de tráfego para um recurso entre em vigor ao mesmo tempo. Ou seja, apenas uma mudança zonal iniciada pelo cliente, uma mudança zonal executada na prática (iniciada por AWS ou por um cliente) ou uma mudança automática para o recurso podem estar ativamente afastando o tráfego 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 Precedência de mudanças zonais.

Identificador do recurso

O identificador de um recurso para o qual habilitar o deslocamento automático zonal, que é o Amazon Resource Name (ARN) do recurso. Você só pode ativar o deslocamento automático zonal para recursos em sua conta que estejam em um AWS serviço compatível com o ARC.

Atributos gerenciados

Os Application Load Balancers registram recursos automaticamente com o ARC para o deslocamento automático zonal. Você deve optar manualmente por outros recursos para o deslocamento automático zonal.

Nome do recurso

O nome de um recurso gerenciado no 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 um é aplicado, ou seja, 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.

Tipo de turno

Define o tipo de deslocamento zonal. Os turnos zonais podem ter um dos seguintes tipos:

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- PRACTICE_RUN
- EXPERIMENTO FIS_

Planos de dados e controle para mudança automática zonal

Ao planejar o failover e a recuperação de desastres, considere a resiliência de seus mecanismos de failover. Recomendamos que você certifique-se de que os mecanismos dos quais você depende durante o failover estejam altamente disponíveis, para que você possa usá-los quando precisar deles em um cenário de desastre. Normalmente, você deve usar funções de plano de dados para seus mecanismos sempre que possível, para obter maior confiabilidade e tolerância a falhas. Com isso em mente, é importante entender como a funcionalidade de um serviço é dividida entre ambientes de gerenciamento e planos de dados e quando você pode confiar em uma expectativa de extrema confiabilidade com o plano de dados de um serviço.

Em geral, um ambiente de gerenciamento 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 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.

Preços do deslocamento automático zonal no ARC

Para o deslocamento automático zonal, AWS desvia o tráfego de uma zona de disponibilidade em seu nome para os recursos suportados 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 obter informações detalhadas sobre preços do ARC e exemplos de preços, consulte Preços do ARC.

Práticas recomendadas ao configurar o deslocamento automático zonal

Esteja ciente das seguintes melhores práticas e considerações ao habilitar o deslocamento automático zonal no Amazon Application Recovery Controller (ARC).

O deslocamento automático zonal inclui dois tipos de turnos de tráfego: turnos automáticos e turnos zonais de execução prática.

- Com um deslocamento automático, AWS ajuda a reduzir seu tempo de recuperação ao afastar o tráfego de recursos do aplicativo de uma zona de disponibilidade durante eventos, em seu nome.
- Com os treinos, o ARC inicia um turno zonal em seu nome ou você inicia um treino de turno zonal. O turno zonal executado AWS na prática transfere o tráfego de uma zona de disponibilidade para um recurso e vice-versa, em um ritmo 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 práticas recomendadas e considerações a serem lembradas com os turnos automáticos e os treinos. Analise os tópicos a seguir antes de habilitar a mudança automática de zona ou configurar execuções práticas para um recurso.

Tópicos

- Limite o tempo em que os clientes permanecem conectados aos seus endpoints
- Pré-escale sua capacidade de recursos e teste a mudança de tráfego
- Esteja ciente dos tipos e restrições de recursos
- Especifique alarmes para treinos
- Avalie os resultados dos treinos

Limite o tempo em que os clientes permanecem conectados aos seus endpoints

Quando o Amazon Application Recovery Controller (ARC) afasta o tráfego de uma deficiência, por exemplo, usando a mudança zonal ou a mudança automática zonal, o mecanismo que o ARC usa para mover o tráfego do seu aplicativo é uma atualização de DNS. Uma atualização de DNS faz com que todas as novas conexões sejam direcionadas para fora do local danificado. No entanto, clientes com conexões abertas preexistentes podem continuar fazendo solicitações no local danificado até que os clientes se reconectem. Para garantir uma recuperação rápida, recomendamos que você limite a quantidade de tempo que os clientes permanecem conectados aos seus endpoints.

Se você usar um Application Load Balancer, poderá usar a `keepalive` opção para configurar por quanto tempo as conexões continuarão. Sugerimos que você reduza o `keepalive` valor para estar alinhado com a meta de tempo de recuperação do aplicativo, por exemplo, 300 segundos. Ao escolher um `keepalive` horário, considere que esse valor é uma troca entre se reconectar com mais frequência em geral, o que pode afetar a latência, e afastar mais rapidamente todos os clientes de uma AZ ou região com problemas.

Para obter mais informações sobre como definir a `keepalive` opção para o Application Load Balancer, consulte a duração da manutenção da atividade do cliente HTTP no Guia do usuário do Application Load Balancer.

Pré-escale sua capacidade de recursos e teste a mudança de tráfego

Ao AWS transferir o tráfego de uma zona de disponibilidade para uma mudança zonal ou automática, é importante que as demais zonas de disponibilidade possam atender ao aumento das taxas de solicitação do seu 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 o tráfego AWS sai de uma zona de disponibilidade — com um deslocamento automático ou durante uma execução prática — ainda AWS pode atender aos clientes do seu aplicativo com o total restante de 30 instâncias, em duas zonas de disponibilidade.

O recurso de deslocamento automático zonal no ARC ajuda você a se recuperar rapidamente de AWS eventos em uma zona de disponibilidade quando você tem um aplicativo com recursos pré-escalados 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. Execute suas próprias execuções práticas sob demanda para ajudar a garantir que sua configuração seja dimensionada adequadamente. 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 zonal no ARC.

Esteja ciente dos tipos e restrições de recursos

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

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

Especifique alarmes para treinos

Você configura pelo menos um alarme (o alarme de resultado) para exercícios com mudança automática zonal. Opcionalmente, você também pode configurar um segundo alarme (o alarme de bloqueio).

Ao considerar os CloudWatch alarmes que você configura para execuções práticas do 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 AWS Well Architected Framework, que recomenda a implementação de indicadores-chave de desempenho (KPIs) como CloudWatch alarmes. 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 não está mais em um `ALARM` estado, o ARC inicia a execução prática na próxima vez que uma execução prática for agendada para o recurso.
- Para o alarme de bloqueio da execução prática, se você optar por configurá-lo, poderá optar por rastrear uma métrica específica usada para indicar que não deseja que uma corrida AWS prática comece.
- 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.

Avalie os resultados dos treinos

O ARC relata um resultado para cada treino. Depois de um treino, avalie o resultado e determine se você precisa agir. Por exemplo, talvez seja necessário escalar a capacidade ou ajustar a configuração de um alarme.

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:
  - O treino foi encerrado porque AWS iniciou um câmbio automático 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.
  - A execução prática foi encerrada porque uma mudança automática zonal com precedência foi iniciada. Consulte Precedência para mudanças zonais.
- CAPACITY_CHECK_FAILED: A verificação da capacidade balanceada entre as zonas de disponibilidade dos recursos do grupo de balanceamento de carga e Auto Scaling falhou.
- PENDENTE: a execução prática está ativa (em andamento). Ainda não há resultado a ser retornado.

Operações de API de mudança automática de zona

A tabela a seguir lista as operações da API ARC que você pode usar com o deslocamento automático zonal. Para obter exemplos de uso de operações de API de mudança automática zonal com o 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 Exemplos de uso do AWS CLI com mudança automática zonal.

Ação	Usando o console ARC	Usando a API 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 zonal em ARC	Consulte ListAutoshifts
Listar recursos para mudança automática de zona	Consulte Recursos compatíveis	Consulte ListManagedResources
Obter recursos para mudança automática de zona	Consulte Recursos compatíveis	Consulte GetManagedResource
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
Ativar ou desativar a notificação do observador de mudança automática	Consulte Habilitando e trabalhando com o deslocamento automático zonal	Consulte UpdateAutoshiftObserverNotificationStatus
Comece uma corrida de treino	Consulte Iniciando um treino, execute um turno zonal	Consulte StartPracticeRun
Cancelar uma corrida de treino	Consulte Cancelar uma mudança de zona para execução prática	Consulte CancelPracticeRun

Exemplos de uso do AWS CLI com mudança automática zonal

Esta seção mostra exemplos simples de aplicativos de como trabalhar com o deslocamento automático zonal, usando o AWS Command Line Interface para trabalhar com o recurso de mudança automática zonal no Amazon Application Recovery Controller (ARC) usando operações de API. Os exemplos têm como objetivo ajudá-lo a desenvolver uma compreensão básica de como trabalhar com o deslocamento automático zonal usando a CLI.

O deslocamento automático zonal é um recurso do ARC. Com o deslocamento automático zonal, você AWS autoriza a transferência do tráfego de recursos de aplicativos suportados de uma zona de disponibilidade durante eventos, em seu nome, para ajudar a reduzir o tempo de recuperação. Para obter mais informações sobre os recursos que você pode usar com o deslocamento automático zonal, consulte. Recursos compatíveis

O deslocamento automático zonal inclui execuções práticas, que também afastam o tráfego das zonas de disponibilidade, para ajudar a verificar se os deslocamentos automáticos são seguros para seu aplicativo.

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. Para obter mais informações sobre como usar o AWS CLI, consulte a Referência de AWS CLI Comandos.

Conteúdo

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 no mesmo local em Região da AWS que seu recurso está implantado.
- 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"
}
```

Inicie uma corrida prática sob demanda

Você pode iniciar uma mudança zonal de execução prática sob demanda com a CLI usando o comando. `start-practice-run`

Por exemplo, para iniciar uma execução prática para um recurso, use um comando como o seguinte:

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

```
    "awayFrom": "usw2-az1",
```

```
{
    "awayFrom": "usw2-az1",
    "comment": "Practice run started. Shifting traffic away from Availability Zone
 usw2-az1.",
}
```

Cancelar uma execução prática em andamento

Você pode cancelar uma execução prática em andamento com a CLI usando `cancel-practice-run` o comando.

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

```
aws arc-zonal-shift cancel-practice-run \
   --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 canceled"
}
```

Cancelar uma mudança automática em andamento

Você pode cancelar um deslocamento automático em andamento com a CLI cancelando o deslocamento automático zonal do recurso. Para cancelar um deslocamento automático zonal, use o. `cancel-zonal-shift command`

```
aws arc-zonal-shift cancel-zonal-shift --zonal-shift-id
 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
```

```
    "awayFrom": "usw2-az1",
    "comment": "Zonal autoshift started. Shifting traffic away from Availability Zone
 usw2-az1.",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Editar uma configuração de execução prática

Você pode editar uma configuração de execução prática para um recurso com a CLI para atualizar diferentes opções de configuração, como alterar os alarmes para execuções de prática ou atualizar as datas bloqueadas ou janelas bloqueadas, quando o ARC não inicia as execuções de prática. 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 no mesmo local em Região da AWS que seu recurso está implantado.
- 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"
}
```

Habilitando e trabalhando com o deslocamento automático zonal

Esta seção fornece procedimentos para trabalhar com mudanças automáticas zonais no Amazon Application Recovery Controller (ARC). Depois de habilitar o deslocamento automático zonal, você pode fazer alterações nas configurações da execução prática, iniciar uma execução prática sob demanda, cancelar um turno em andamento, incluindo execuções de treino, ou ativar as notificações do observador do deslocamento automático.

Habilitar ou desabilitar a mudança automática de zona

As etapas aqui explicam como ativar ou desativar o deslocamento automático zonal no console do Amazon Application Recovery Controller (ARC). 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 zonal está ativada, você AWS autoriza a desviar o tráfego de recursos do aplicativo 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 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 Ativar mudança automática zonal 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.

Conteúdo

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 Amazon Application Recovery Controller (ARC). 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 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. Escolha desativar o deslocamento automático zonal se não quiser AWS iniciar um deslocamento automático para um recurso quando houver um evento. 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 Práticas recomendadas ao configurar o deslocamento automático zonal.
7. Opcionalmente, especifique datas e janelas bloqueadas. Escolha datas ou janelas (dias e horários) para impedir que o ARC inicie os treinos deste 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. Escolha Criar.

Como editar uma configuração de execução prática

1. Abra o console ARC 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 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.

Cancelamento de um deslocamento automático zonal

Para interromper um deslocamento automático zonal em andamento para um recurso, você deve cancelar o deslocamento automático zonal.

Para interromper um deslocamento automático zonal em andamento

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

Iniciando um treino, execute um turno zonal

As etapas desta seção explicam como iniciar uma mudança zonal de execução prática sob demanda no console ARC. 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 iniciar um deslocamento zonal de execução prática depois de configurar o deslocamento automático zonal e criar uma configuração de execução prática.

Para iniciar uma prática, execute o turno zonal

1. Abra o console ARC emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança automática de zona.
3. Em Recursos de mudança automática zonal, navegue até um recurso individual que tenha o deslocamento automático zonal configurado.
4. Na página de visão geral do recurso, escolha Iniciar execução prática.
5. Selecione uma zona de disponibilidade e, em seguida, insira um comentário para sua execução prática. A execução prática afastará o tráfego da Zona de Disponibilidade que você selecionou.
6. Escolha Iniciar.

Cancelar uma mudança de zona para execução prática

As etapas desta seção explicam como cancelar uma mudança de zona no console ARC. 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 turnos zonais ou praticar corridas que você mesmo inicia. Você também pode cancelar os turnos zonais que AWS começam como recurso para uma execução prática de mudança automática zonal.

Como cancelar uma mudança de zona para execução prática

1. Abra o console ARC emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Multi-AZ, escolha Mudança de zona.
3. Selecione um turno zonal de execução de treino que você deseja cancelar e, em seguida, escolha Cancelar turno zonal ou Cancelar execução de treino.

4. Na caixa de diálogo modal de confirmação, escolha Confirmar.

Ativando ou desativando a notificação do observador de deslocamento automático

Você pode configurar o deslocamento automático zonal para notificá-lo, por meio da Amazon EventBridge, sempre que AWS iniciar um deslocamento automático para afastar o tráfego de uma zona de disponibilidade potencialmente prejudicada. Você deve configurar essa opção em cada uma Região da AWS das quais deseja receber notificações. Você não precisa configurar nenhum recurso específico com o deslocamento automático zonal para ativar essas notificações separadas. Para obter mais informações, consulte Usando o deslocamento automático zonal com a Amazon EventBridge.

As etapas desta seção explicam como ativar a notificação do observador de mudança automática usando o console do Amazon Application Recovery Controller (ARC). 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.

Para ativar ou desativar a notificação do observador de mudança automática

1. Abra o console ARC emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Em Introdução, escolha Ativar notificação do observador de mudança automática.
3. Na caixa de diálogo de confirmação, escolha Habilitar notificação do observador.

Testando o deslocamento automático zonal com AWS FIS

Você pode usar AWS Fault Injection Service para configurar e executar experimentos que ajudam a simular condições do mundo real, como o cenário Disponibilidade de AZ: Interrupção de Energia, que demonstrará o que acontece quando AWS inicia uma mudança automática zonal em seus recursos habilitados para mudança automática durante uma deficiência potencialmente generalizada do AZ.

A ação de início de `aws:arc:start-zonal-autoshift` recuperação permite que você demonstre como AWS transferirá automaticamente o tráfego, para recursos habilitados para o deslocamento automático zonal, de uma AZ potencialmente prejudicada e os redirecionará para a integridade da mesma Região da AWS durante a execução do cenário de disponibilidade da AZ. AZs

Por exemplo, você pode usar a biblioteca de AWS FIS cenários para simular uma deficiência no AZ causada por uma interrupção de energia. Neste experimento, cinco minutos após o início da

interrupção da alimentação do AZ, a ação de recuperação desvia `aws:arc:start-zonal-autoshift` automaticamente o tráfego de recursos do AZ especificado. O tráfego é deslocado pelos 25 minutos restantes da interrupção de energia, para demonstrar como a mudança automática seria acionada quando houvesse uma deficiência potencialmente generalizada do AZ. Quando o experimento é concluído, a mudança de tráfego termina e o tráfego começa a fluir para todos AZs novamente. Esse processo demonstra uma recuperação completa de um evento de energia que afeta uma AZ.

Como os experimentos diferem das execuções práticas de mudança automática zonal

AWS FIS os experimentos diferem das execuções práticas de deslocamento automático zonal porque, durante as execuções práticas, o ARC desvia o tráfego do seu recurso de uma AZ como parte de um processo normal para garantir que seu aplicativo possa tolerar a perda de uma AZ. No entanto, durante um AWS FIS experimento, AWS FIS demonstra como uma deficiência de AZ e uma mudança automática seriam acionadas para seus recursos habilitados para a mudança automática em seu nome e, em seguida, cancelaria a mudança automática quando a deficiência fosse resolvida.

Você não pode atualizar uma mudança de zona AWS iniciada pelo FIS enquanto ela está em execução. Além disso, se você cancelar uma mudança de zona externa AWS FIS, o AWS FIS experimento será encerrado.

AWS FIS mecanismo de segurança baseado na expiração

AWS FIS gerencia a mudança zonal usando as operações de StartZonalShiftUpdateZonalShift, e CancelZonalShiftAPI, com o `expiresIn` campo para essas solicitações definido como 1 minuto como mecanismo de segurança. Isso permite AWS FIS reverter rapidamente a mudança de zona se houver eventos inesperados, como interrupções na rede ou problemas no sistema. No console ARC, o campo de tempo de expiração será exibido AWS FIS-managed, e a expiração real esperada será determinada pela duração especificada na ação de mudança zonal. Para obter mais informações sobre corridas práticas, consulte Como funcionam o deslocamento automático zonal e as corridas práticas

Não pode haver mais do que um deslocamento zonal aplicado em um determinado momento. Ou seja, apenas uma prática executa mudança zonal, mudança zonal iniciada pelo cliente, mudança automática ou AWS FIS experimento para o recurso. Quando uma segunda mudança zonal é iniciada, o ARC segue uma precedência para determinar qual tipo de mudança zonal está em vigor para um recurso. Para obter mais informações sobre a precedência de mudanças zonais, consulte. Precedência para mudanças zonais

Para obter mais informações sobre ações de AWS FIS recuperação, consulte a ação de AWS FIS recuperação no Guia AWS Fault Injection Service do usuário.

Registro e monitoramento para mudança automática zonal no Amazon Application Recovery Controller (ARC)

Você pode usar AWS CloudTrail a Amazon EventBridge para monitorar o deslocamento automático zonal no Amazon Application Recovery Controller (ARC), para analisar padrões e ajudar a solucionar problemas.

Tópicos

Registrando chamadas de API de mudança automática zonal usando AWS CloudTrail

O deslocamento automático zonal para ARC é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no ARC. CloudTrail captura todas as chamadas de API para mudança de zona como eventos. As chamadas capturadas incluem chamadas do console ARC e chamadas de código para as operações da API ARC para mudança de zona.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para mudança de zona. 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 ARC para mudança de zona, 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 de mudança automática zonal em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no ARC para mudança automática zonal, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos de mudança automática zonal no 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 eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do ARC são registradas CloudTrail e documentadas no Guia de referência da API Routing Control para o Amazon Application Recovery Controller. Por exemplo, chamadas para as `ListManagedResources` ações `StartZonalShift` e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Visualizando eventos ARC no histórico de eventos

CloudTrail permite que você visualize eventos recentes no histórico de eventos. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário.

Compreendendo as entradas do arquivo de log de deslocamento automático zonal

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 `ListManagedResources` ação do deslocamento automático 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"
    }
  }
```

Usando o deslocamento automático zonal com a Amazon EventBridge

Usando a Amazon EventBridge, você pode configurar regras orientadas por eventos que monitoram seus recursos de mudança automática zonal 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 começa para o deslocamento automático zonal.

Você pode criar regras na Amazon EventBridge para agir no deslocamento automático zonal. Um evento para mudança automática zonal especifica informações de status sobre execuções de treino ou turnos automáticos, por exemplo, quando uma execução prática é iniciada. Você pode configurar o deslocamento automático zonal para notificá-lo sobre eventos de mudança automática zonal para recursos que você habilita para o serviço.

Você também pode escolher, além ou em vez de outras notificações, ativar a notificação de deslocamento automático do observador, que fornece um evento de notificação sempre que AWS inicia um deslocamento automático para uma zona de disponibilidade potencialmente comprometida. A notificação do observador do Autoshift é separada das notificações que você recebe quando o tráfego dos recursos que você ativou para o deslocamento automático zonal é deslocado de uma zona de disponibilidade. Você não precisa configurar nenhum recurso com o deslocamento automático zonal para ativar a notificação do observador do deslocamento automático. Para obter mais informações, consulte Habilitando e trabalhando com o deslocamento automático zonal.

Para capturar eventos de deslocamento automático zonal específicos 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 ARC para quase EventBridge em tempo real, sob 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 de mudança automática zonal com EventBridge

Com EventBridge, você pode criar regras que definem ações a serem tomadas quando o ARC emite eventos para seus recursos. Por exemplo, você pode criar uma regra que envia uma mensagem de e-mail quando uma execução prática é iniciada para o deslocamento automático zonal.

Para digitar ou copiar e colar um padrão de evento no EventBridge console, selecione a opção Inserir minha própria opção no console. Para ajudá-lo a determinar padrões de eventos que podem ser úteis para você, este tópico inclui exemplos de padrões de correspondência de eventos de deslocamento automático zonal e eventos de deslocamento automático zonal 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 na qual você deseja criar a regra, ou seja, a região na qual você está interessado 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 de mudança automática zonal

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 de deslocamento automático zonal.

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`
- `FIS Experiment Autoshift In Progress`
- `FIS Experiment Autoshift Completed`
- `FIS Experiment Autoshift Canceled`

Quando uma execução prática é interrompida, consulte o campo `additionalFailureInfo` para obter mais informações sobre o que causou a interrupção.

Você pode optar por monitorar todos os AWS turnos automáticos ativando as notificações do observador do deslocamento automático. Depois de ativar a notificação do observador de deslocamento automático, para receber as notificações, escolha ser notificado sobre o tipo de detalhe do deslocamento automático zonal. `Autoshift In Progress` Para ver as etapas para habilitar a notificação do observador de mudança automática, consulte. Habilitando e trabalhando com o deslocamento automático zonal

Para ver exemplos, consulte a seção Exemplos de eventos de mudança automática zonal.

- Selecione todos os eventos do deslocamento automático zonal em que um deslocamento automático foi iniciado.

  Observe o seguinte:

  - Se você tiver a notificação de mudança automática do observador ativada, o ARC retornará todos os eventos de mudança automática.

- Se você não tiver a notificação do observador de deslocamento automático ativada, o ARC retornará eventos de deslocamento automático somente quando um recurso que você configurou para o deslocamento automático zonal for incluído em um deslocamento automático.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Autoshift In Progress"
    ]
}
```

- Selecione todos os eventos do deslocamento automático zonal em que uma corrida prática foi iniciada.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Started"
    ]
}
```

- Selecione todos os eventos do deslocamento automático zonal em que uma execução prática falhou.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Failed"
    ]
}
```

Exemplos de eventos de mudança automática zonal

Esta seção inclui exemplos de eventos para ações de mudança automática zonal.

O seguinte é um exemplo de evento para a `Autoshift In Progress` ação, quando 1) a notificação do observador de deslocamento automático está ativada e 2) você não configurou um recurso com deslocamento automático zonal incluído em um deslocamento automático:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":"AWS has started an autoshift for an impaired Availability Zone.
 This notification
            is separate from autoshift notifications for resources, if any, that you
 have configured for
            zonal autoshift. For details, see the Developer Guide."
        }
    }
}
```

O seguinte é um exemplo de evento para a `Autoshift In Progress` ação, quando 1) a notificação do observador de deslocamento automático está desativada e 2) você configurou um recurso com mudança automática zonal que está incluído em um deslocamento automático:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "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": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

Veja a seguir um exemplo de evento para a `Practice Run Interrupted` ação:

```
{
    "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 para a `FIS Experiment Autoshift In Progress` ação:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "FIS Experiment Autoshift In Progress",
    "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": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

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 ARC, consulte as seções anteriores neste tópico.

4. Na página Selecionar destino, escolha CloudWatchcomo seu alvo.
5. Escolha um grupo de CloudWatch registros no menu suspenso.

Identity and Access Management para mudança automática zonal

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 (conectado) e autorizado (tem permissões) para usar os recursos do ARC. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Conteúdo

Como o deslocamento automático zonal no ARC funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao deslocamento automático zonal no Amazon Application Recovery Controller (ARC), saiba quais recursos do IAM estão disponíveis para uso com o deslocamento automático zonal.

Recursos do IAM que você pode usar com o deslocamento automático zonal no ARC

Atributo do IAM	Suporte para mudança automática zonal
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim

Atributo do IAM	Suporte para mudança automática zonal
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para obter uma visão geral de alto nível de como os AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS Serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para ARC

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 do IAM, grupo de usuários ou perfil. 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 Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim 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 perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Para ver exemplos de políticas baseadas em identidade do ARC, consulte. Exemplos de políticas baseadas em identidade no Amazon Application Recovery Controller (ARC)

Políticas baseadas em recursos no ARC

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos 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 políticas para ARC

Compatível com 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 podem ser usadas 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. Algumas operações também 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 de ações do ARC para mudança automática zonal, consulte Ações definidas pelo Amazon Route 53 Zonal Shift na Referência de Autorização de Serviço.

As ações de política no ARC para mudança automática zonal usam os seguintes prefixos antes da ação:

```
arc-zonal-shift
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas. Por exemplo, o seguinte:

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift: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": "arc-zonal-shift:Describe*"
```

Para ver exemplos de políticas baseadas em identidade ARC para mudança automática zonal, consulte. Exemplos de políticas baseadas em identidade para mudança automática zonal

Recursos de política para mudança automática zonal no ARC

Compatível com 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 de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um 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 você pode especificar com o ARN de cada recurso, consulte o tópico a seguir na Referência de Autorização de Serviço:

- Ações definidas pelo Amazon Route 53 - Zonal Shift

Para ver as ações e os recursos que você pode usar com uma chave de condição, consulte o tópico a seguir na Referência de Autorização de Serviço:

- Chaves de condição definidas pelo Amazon Route 53 - Zonal Shift

Para ver exemplos de políticas baseadas em identidade ARC para mudança automática zonal, consulte. Exemplos de políticas baseadas em identidade para mudança automática zonal

Chaves de condição de política para mudança automática zonal no ARC

Compatível com chaves de condição de política específicas de 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 `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `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 antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar 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 da 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 das chaves de condição ARC para o deslocamento automático zonal, consulte os tópicos a seguir na Referência de Autorização de Serviço:

- 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 pela mudança de zona do Amazon Route 53

Para ver exemplos de políticas baseadas em identidade ARC para mudança automática zonal, consulte. Exemplos de políticas baseadas em identidade para mudança automática zonal

Listas de controle de acesso (ACLs) em ARC

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso baseado em atributos (ABAC) com ARC

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as 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. Marcar de entidades e atributos 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 estiver 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 chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do 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 deslocamento automático zonal no ARC inclui o seguinte suporte parcial para ABAC:

- O deslocamento automático zonal suporta ABAC para recursos gerenciados que são registrados no ARC para mudança zonal. 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.

Usando credenciais temporárias com ARC

Compatível com 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 “Trabalhe 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 funções, consulte Alternar para um perfil do IAM (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 principais entre serviços para ARC

Compatibilidade com o recurso de 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. Permissões concedidas por políticas a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, acionar outra ação em outro serviço. Nesse caso, você precisa ter permissões para executar ambas as ações.

Para ver se uma ação exige ações dependentes adicionais em uma política, consulte o tópico a seguir na Referência de Autorização de Serviço:

- Mudança de zona do Amazon Route 53

Funções de serviço para ARC

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar 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.

Funções vinculadas a serviços para ARC

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções

vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço ARC, consulte. Usando a função vinculada ao serviço para mudança automática zonal no ARC

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para mudança automática zonal

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos ARC. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos 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 aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo ARC, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon Application Recovery Controller (ARC) na Referência de autorização de serviço. ARNs

Tópicos

- Práticas recomendadas de política
- Exemplo: acesso ao console de mudança automática zonal
- Exemplos: ações da API ARC

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos ARC em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance 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 funções 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 da 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 cem verificações de política e recomendações práticas para ajudar 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 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 de mudança automática zonal

Para acessar o console do Amazon Application Recovery Controller (ARC), você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do ARC em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva 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 à operação de API que estiverem tentando executar.

Para realizar algumas tarefas, os usuários devem ter permissão para criar a função vinculada ao serviço associada ao deslocamento automático zonal no ARC. Para saber mais, consulte Usando a função vinculada ao serviço para mudança automática zonal no ARC.

Para dar aos usuários acesso total ao uso do deslocamento automático zonal no AWS Management Console, 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",
                  "arc-zonal-shift:CreatePracticeRunConfiguration",
                  "arc-zonal-shift:DeletePracticeRunConfiguration",
                  "arc-zonal-shift:ListAutoshifts",
                  "arc-zonal-shift:UpdatePracticeRunConfiguration",
                  "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:DescribeAlarms",
            "Resource": "*"
        }
    ]
}
```

Exemplos: ações da API ARC

Você pode usar uma política para garantir que um usuário possa usar as ações da API ARC para o deslocamento automático zonal para configurar o deslocamento automático zonal de forma que AWS transfira o tráfego de recursos do aplicativo de uma zona de disponibilidade, em seu nome, para saudável AZs na Região da AWS, para ajudar a reduzir o tempo de recuperação durante eventos. Para fornecer essas permissões, 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 permissões para a função vinculada ao serviço associada ao ARC. As permissões necessárias para criar a função vinculada ao serviço estão incluídas no exemplo de política a seguir. Para saber mais, consulte Usando a função vinculada ao serviço para mudança automática zonal no ARC.

Para trabalhar com operações de API para mudança automática zonal, 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",
                   "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",
                    "health:DescribeEvents"
            ],
            "Resource" : "*"
        },
        {
            "Effect" : "Allow",
            "Action" : [
                    "arc-zonal-shift:CancelZonalShift",
                    "arc-zonal-shift:GetManagedResource",
                    "arc-zonal-shift:StartZonalShift",
                    "arc-zonal-shift:UpdateZonalShift"
            ],
            "Resource" : "*"
        }
    ]
}
```

Usando a função vinculada ao serviço para mudança automática zonal no ARC

O deslocamento automático zonal no Amazon Application Recovery Controller usa uma função vinculada ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a um serviço — nesse caso, ARC. A função vinculada ao serviço é predefinida pelo ARC e inclui todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome para fins específicos.

Uma função vinculada ao serviço facilita a configuração do ARC porque você não precisa adicionar manualmente as permissões necessárias. O ARC define as permissões para a função vinculada ao serviço e, a menos que seja definido de outra forma, somente o ARC pode assumir suas funções. 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 de mudança automática zonal do ARC porque você não pode remover inadvertidamente a permissão 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 para esse serviço.

Permissões de função vinculadas ao serviço para AWSService RoleForZonalAutoshiftPracticeRun

O 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 AWSService RoleForZonalAutoshiftPracticeRun

Esse perfil vinculado 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`

Para visualizar as permissões para esta política, consulte AWSZonalAutoshiftPracticeRunSLRPolicy na Referência de políticas gerenciadas pela AWS .

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Criando a função AWSServiceRoleForZonalAutoshiftPracticeRunvinculada ao serviço para ARC

Você não precisa criar manualmente a função vinculada a serviço AWSServiceRoleForZonalAutoshiftPracticeRun. Quando você cria a configuração da primeira execução prática no AWS Management Console, no ou em um AWS SDK AWS CLI, o ARC cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria a configuração da primeira execução prática, o ARC cria a função vinculada ao serviço para você novamente.

Editando a função AWSServiceRoleForZonalAutoshiftPracticeRunvinculada ao serviço para ARC

O 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 obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo a função AWSServiceRoleForZonalAutoshiftPracticeRunvinculada ao serviço para ARC

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de 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 zonal no ARC.

> **Note**
>
> Se o serviço ARC estiver usando a função quando você tentar excluir os recursos, a exclusão da função 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 AWSService RoleForZonalAutoshiftPracticeRun vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Atualizações na função vinculada ao serviço ARC para deslocamento automático zonal

Para atualizações das políticas AWS gerenciadas para as funções vinculadas ao serviço ARC, consulte a tabela de atualizações de políticas AWS gerenciadas para ARC. Você também pode se inscrever para receber alertas automáticos de RSS na página de histórico do documento ARC.

AWS políticas gerenciadas para mudança automática zonal no Amazon Application Recovery Controller (ARC)

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 elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AWS política gerenciada: AWSZonal AutoshiftPracticeRun SLRPolicy

Não é possível anexar a `AWSZonalAutoshiftPracticeRunSLRPolicy` às entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite que o Amazon Application Recovery Controller (ARC) faça o seguinte para o deslocamento automático zonal:

- 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)
- Gerencie verificações de capacidade balanceada para treinos e turnos automáticos

Para obter mais informações, consulte Usando a função vinculada ao serviço para mudança automática zonal no ARC.

Atualizações para políticas AWS gerenciadas para mudança automática zonal

Para obter detalhes sobre as atualizações das políticas AWS gerenciadas para mudança automática zonal no ARC desde que esse serviço começou a rastrear essas alterações, consulte. Atualizações nas políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC) Para alertas automáticos sobre alterações nesta página, assine o feed RSS na página de histórico do documento ARC.

Use o controle de roteamento para recuperar aplicativos multirregionais no ARC

Esta seção explica como usar o recurso de controle de roteamento no Amazon Application Recovery Controller (ARC) para minimizar interrupções e ajudar a fornecer continuidade aos seus usuários quando você tem um AWS aplicativo implantado em vários. Regiões da AWS

Você também pode aprender sobre a verificação de prontidão, um recurso do ARC que você pode usar para obter informações sobre se seus aplicativos e recursos estão preparados para recuperação.

Os tópicos desta seção descrevem os recursos de controle de roteamento e verificação de prontidão, como configurá-los e como usá-los.

Tópicos

Controle de roteamento no ARC

Para transferir tráfego para várias réplicas de aplicativos Regiões da AWS, você pode usar controles de roteamento no Amazon Application Recovery Controller (ARC) que são integrados a um tipo específico de verificação de saúde 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 regional 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 seus aplicativos em cada região.

Esta seção explica como o controle de roteamento funciona, como configurar componentes de controle de roteamento e como usá-los para redirecionar o tráfego para failover.

Os componentes de controle de roteamento no 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 ARC cria para seu cluster ou criar seus próprios painéis de controle personalizados. É

necessário criar um cluster antes de criar um painel de controle ou um controle de roteamento. Cada cluster no 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 o controle de roteamento 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 AWS CLI ou (recomendado) ou usando o. AWS Management Console

Esta seção explica como os controles de roteamento funcionam e como criá-los e usá-los para redirecionar o tráfego para seu aplicativo.

> **Important**
>
> Para saber como se preparar para usar o ARC para redirecionar o tráfego como parte de um plano de failover para seu aplicativo em um cenário de desastre, consulte. Melhores práticas para controle de roteamento no ARC

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 `0ff` (para interromper o fluxo de tráfego para uma célula) e atualizando outro estado de controle de roteamento para 0n (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 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 AWS serviço 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 para controle de roteamento, para garantir que o redirecionamento do tráfego usando controles de roteamento não prejudique a disponibilidade. Para obter mais informações, consulte Criação de regras de segurança para controle de roteamento .

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.

Como usar o controle de roteamento

Para atualizar um estado de controle de roteamento, para que você possa redirecionar o tráfego, você deve se conectar a um dos endpoints do cluster no 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 ARC junto com as verificações de integridade e conjuntos de registros DNS do Route 53, usando registros DNS com políticas de roteamento ponderadas. Para ver um exemplo detalhado, consulte a seção sobre failover de tráfego de usuários na seguinte postagem do AWS blog: Criação de aplicativos altamente resilientes usando o Amazon Application Recovery Controller (ARC), Parte 2: pilha multirregional

Quando você inicia um failover para um controle de roteamento de Região da AWS uso, devido às etapas envolvidas no fluxo de tráfego, talvez você não veja o tráfego sair da região imediatamente. Também pode levar pouco tempo para que as conexões existentes e em andamento na região sejam concluídas, dependendo do comportamento do cliente e da reutilização da conexão.

Dependendo das configurações de DNS e de outros fatores, as conexões existentes podem ser concluídas em apenas alguns minutos ou levar mais tempo. Para obter mais informações, consulte Garantir que os turnos de trânsito terminem rapidamente.

Benefícios do controle de roteamento

Um controle de roteamento no 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 EC2 instâncias da Amazon, com base em verificações de saúde em nível de recursos.
- 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.

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 em. 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 a réplica ativa apresenta falhas, você pode redirecionar o tráfego do usuário para lá para restaurar a disponibilidade do aplicativo. Você deve decidir se deseja remover ou corrigir uma réplica com base nas informações de seus sistemas de monitoramento e verificação de integridade.

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

AWS Disponibilidade da região para controle de roteamento

Para obter informações detalhadas sobre endpoints regionais de suporte e serviço para o Amazon Application Recovery Controller (ARC), consulte os endpoints e cotas do Amazon Application Recovery Controller (ARC) na Referência geral da Amazon Web Services.

> **Note**
>
> O controle de roteamento no Amazon Application Recovery Controller (ARC) é um recurso global. No entanto, você deve especificar a região Oeste dos EUA (Oregon) (especificar o parâmetro`--region us-west-2`) nos AWS CLI comandos regionais do ARC. Ou seja, quando você cria recursos como clusters, painéis de controle ou controles de roteamento.

Um controle de roteamento ARC é um on/off switch que altera o estado de uma verificação de integridade do 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 réplica principal para, por exemplo, uma réplica em espera. Ao usar as operações altamente confiáveis da API do plano de dados ARC para fazer consultas de controle de roteamento e atualizações do estado do controle de roteamento, você pode confiar no ARC para failover durante cenários de recuperação de desastres. Para obter mais informações, consulte Obter e atualizar estados de controle de roteamento usando a API ARC (recomendado).

O ARC mantém os estados de controle de roteamento em um cluster, que é um conjunto de cinco endpoints regionais redundantes. O ARC propaga mudanças no estado do controle de roteamento em todo o cluster, que está localizado em uma EC2 frota da Amazon, para obter um quórum em cinco regiões. AWS Após a propagação, quando você consulta o ARC para obter 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 ARC propaga a atualização pelas cinco regiões do cluster.

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

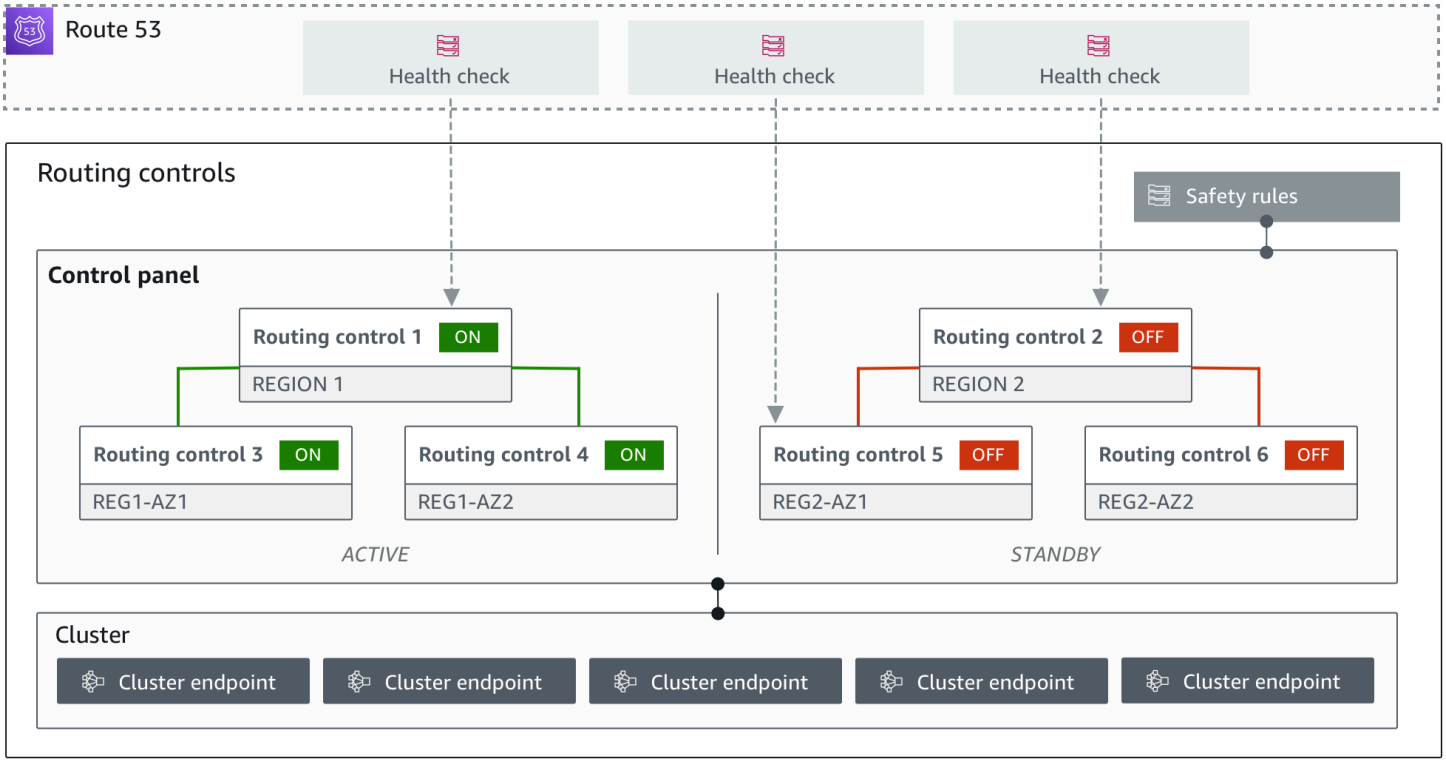
O ARC oferece extrema confiabilidade com seu plano de dados para que você faça o failover manual de seu aplicativo em todas as células. O ARC garante que pelo menos três dos cinco endpoints do cluster estejam sempre acessíveis para você realizar alterações no estado do controle de roteamento. Observe que cada cluster 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).

Componentes do controle de roteamento

O diagrama a seguir ilustra um exemplo de componentes que suportam o recurso de controle de roteamento no 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 ARC altera as verificações de saúde 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 na abertura e outras consequências não intencionais.



A seguir estão os componentes do recurso de controle de roteamento no 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 on/off switch simples, hospedado em um cluster, que você usa para controlar o roteamento do tráfego do cliente para dentro e para fora das células. Ao criar um controle de roteamento, você adiciona uma verificação de integridade do ARC no Route 53. Isso permite que você redirecione o tráfego (usando as verificações de saúde, configuradas com registros DNS para seus aplicativos) ao atualizar o estado do controle de roteamento no ARC.

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 do controle de

roteamento, o ARC atualiza as verificações de integridade correspondentes, que redirecionam o tráfego — por exemplo, para fazer o failover para 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 na abertura” não intencionais.

Painel de controle padrão

Quando você cria um cluster, o 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

Regras de segurança são regras que você adiciona ao controle de roteamento 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 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 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.

Planos de dados e controle para controle de roteamento

Ao planejar o failover e a recuperação de desastres, considere a resiliência de seus mecanismos de failover. Recomendamos que você certifique-se de que os mecanismos dos quais você depende durante o failover estejam altamente disponíveis, para que você possa usá-los quando precisar deles em um cenário de desastre. Normalmente, você deve usar funções de plano de dados para seus mecanismos sempre que possível, 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 ambientes de gerenciamento e planos de dados e quando você pode confiar em uma expectativa de extrema confiabilidade com o plano de dados de um serviço.

Como acontece com a maioria dos AWS serviços, a funcionalidade do recurso de controle de roteamento é suportada por planos de controle e planos de dados. Embora ambos tenham sido criados para serem confiáveis, um plano de controle é otimizado para consistência de dados, enquanto um plano de dados é otimizado para disponibilidade. Um plano de dados é projetado para ser resistente e manter a disponibilidade mesmo durante eventos de ruptura, quando um ambiente de gerenciamento pode ficar indisponível.

Em geral, um ambiente de gerenciamento 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. Por isso, recomendamos que você use operações de planos de dados quando a disponibilidade for importante, por exemplo, quando precisar redirecionar o tráfego para uma réplica em espera durante uma interrupção.

Para controle de roteamento, os planos de controle e os planos de dados são divididos da seguinte forma:

- A API do plano de controle para controle de roteamento é a API de configuração do controle de recuperação, suportada 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 ambiente de gerenciamento da configuração do controle de roteamento não é altamente disponível.
- O plano de dados de controle de roteamento é um cluster dedicado em cinco regiões geograficamente isoladas AWS . Cada cliente cria um ou mais clusters usando o ambiente de gerenciamento 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.

Como o plano de dados de controle de roteamento está altamente disponível, recomendamos que você planeje usar o AWS Command Line Interface para fazer chamadas de API para trabalhar com estados de controle de roteamento quando quiser fazer o failover para se recuperar de um evento. Para obter mais informações sobre as principais considerações ao preparar e concluir uma operação de recuperação com controle de roteamento, consulte. Melhores práticas para controle de roteamento no ARC

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.

Marcação para controle de roteamento no Amazon Application Recovery Controller (ARC)

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 no controle de roteamento no ARC:

- Clusters
- Painéis de controle
- Regras de segurança

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

A seguir estão exemplos de marcação no controle de roteamento usando o. AWS CLI

```
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
```

Para obter mais informações, consulte TagResourceo Guia de referência da API Recovery Control Configuration para o Amazon Application Recovery Controller (ARC).

Preços para controle de roteamento no ARC

Para controle de roteamento no ARC, 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 ajudar a gerenciar custos e melhorar a eficiência, você pode configurar o compartilhamento entre contas para um cluster, para compartilhar um cluster com várias AWS contas. Para obter mais informações, consulte Support cross-account para clusters no ARC.

Para obter informações detalhadas sobre preços do ARC e exemplos de preços, consulte Preços do ARC.

Introdução à recuperação multirregional no Amazon Application Recovery Controller (ARC)

Para fazer o failover de seus aplicativos usando o controle de roteamento no Amazon Application Recovery Controller (ARC), você deve ter AWS aplicativos que estejam em vários Regiões da AWS. Para começar, primeiro, certifique-se de que seus aplicativos estejam configurados em réplicas em silos em cada região, para que você possa passar de um para outro durante um evento. Em seguida, você pode criar controles de roteamento para redirecionar o tráfego do aplicativo para o failover de um aplicativo primário para um secundário, mantendo a continuidade para seus usuários.

> **Note**
>
> Se você tiver um aplicativo isolado por zonas de disponibilidade, considere usar o deslocamento zonal ou o deslocamento automático zonal para recuperação de failover. Nenhuma configuração é necessária para usar o deslocamento zonal ou o deslocamento automático zonal para recuperar de forma confiável os aplicativos das deficiências da Zona de Disponibilidade. Para obter mais informações, consulte Use o deslocamento zonal e o deslocamento automático zonal para recuperar aplicativos no ARC.

Para que você possa usar o controle de roteamento ARC para recuperar aplicativos durante um evento, recomendamos que você configure pelo menos dois aplicativos que sejam réplicas um do outro. Cada réplica, ou célula, representa uma Região da AWS. Depois de configurar os recursos do aplicativo para se alinharem às regiões, certifique-se de que seu aplicativo esteja configurado para uma recuperação bem-sucedida seguindo as etapas a seguir.

Dica: 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. Para saber mais e baixar os modelos, consulteConfigurando um aplicativo de exemplo.

Para se preparar para usar o controle de roteamento, certifique-se de que seu aplicativo esteja configurado para ser resiliente fazendo o seguinte:

1. Crie cópias independentes de sua pilha de aplicativos (camada de rede e computação) que sejam réplicas umas das outras em cada região para que você possa transferir o tráfego de uma para a outra quando houver um evento. Certifique-se de que você não tenha nenhuma dependência entre regiões no código do aplicativo que faria com que a falha de uma réplica afetasse a outra. Para que o failover entre eles seja bem-sucedido Regiões da AWS, seus limites de pilha devem estar dentro de uma região.
2. Duplique todos os dados de estado necessários para seu aplicativo nas réplicas. Você pode usar serviços AWS de banco de dados para ajudar a replicar seus dados.

Comece a usar o controle de roteamento para falha de tráfego

O controle de roteamento no Amazon Application Recovery Controller (ARC) permite que você acione o failover para que seu tráfego passe entre cópias redundantes de aplicativos, ou réplicas, que estão sendo executadas separadamente. Regiões da AWS O failover é executado com o DNS, usando o plano de dados do Amazon Route 53.

Depois de configurar suas réplicas em cada região, conforme descrito na próxima seção, você pode associar cada uma a um controle de roteamento. Primeiro, você associa os controles de roteamento aos nomes de domínio de nível superior de suas réplicas em cada região. Em seguida, você adiciona uma verificação de integridade do controle de roteamento ao controle de roteamento para que ele possa ativar e desativar o fluxo de tráfego. Isso permite que você controle o roteamento de tráfego entre réplicas do seu aplicativo.

Você pode atualizar os estados de controle de roteamento no AWS Management Console tráfego de failover, mas recomendamos que, em vez disso, use ações ARC, usando a API ou AWS CLI alterando-as. As ações da API não dependem do console, então elas são mais resilientes.

Por exemplo, para fazer o failover entre regiões, de us-west-1 a us-east-1, você pode `update-routing-control-state` usar a ação da API para definir o estado de para e para. `us-west-1` `Off` `us-east-1` `On`

Antes de criar componentes de controle de roteamento para configurar o failover para seu aplicativo, certifique-se de que seu aplicativo esteja dividido em réplicas regionais, para que você possa fazer o failover de uma para a outra. Para saber mais e começar a isolar um novo aplicativo ou criar uma pilha de exemplos, consulte as próximas seções.

Configurando um aplicativo de exemplo

Para ajudá-lo a entender como o controle de roteamento funciona, fornecemos um exemplo de aplicativo chamado`TicTacToe`. O exemplo usa AWS CloudFormation modelos para simplificar o processo, bem como um AWS CloudFormation modelo disponível para download para que você mesmo possa explorar rapidamente a configuração e o uso do ARC.

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

Para começar a usar um aplicativo e AWS CloudFormation modelos de amostra, consulte as instruções do README no repositório ARC GitHub. Você pode aprender mais sobre o uso AWS CloudFormation de modelos lendo AWS CloudFormation os conceitos no Guia AWS CloudFormation do usuário.

Melhores práticas para controle de roteamento no ARC

Recomendamos as seguintes melhores práticas para recuperação e preparação para failover para controle de roteamento no ARC.

Tópicos

- Mantenha as AWS credenciais personalizadas e de longa duração seguras e sempre acessíveis
- Escolha valores de TTL mais baixos para registros DNS envolvidos no failover
- Limite o tempo em que os clientes permanecem conectados aos seus endpoints

- Marque ou codifique seus cinco endpoints de cluster regionais e controle de roteamento ARNs
- Escolha um de seus endpoints aleatoriamente para atualizar seus estados de controle de roteamento
- Use a API de plano de dados extremamente confiável para listar e atualizar os estados de controle de roteamento, não o console

Mantenha as AWS credenciais 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 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, você pode gerenciar centralmente as credenciais de segurança, como chaves de acesso e permissões de acesso aos AWS recursos. 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 ARC com a API do plano de dados do cluster de recuperação, você pode anexar uma política do ARC IAM ao seu usuário. Para saber mais, consulte Exemplos de políticas baseadas em identidade no Amazon Application Recovery Controller (ARC).

Escolha valores de TTL mais baixos para registros 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.

Limite o tempo em que os clientes permanecem conectados aos seus endpoints

Quando você usa controles de roteamento para mudar de um Região da AWS para outro, o mecanismo que o Amazon Application Recovery Controller (ARC) usa para mover o tráfego

do seu aplicativo é uma atualização de DNS. Essa atualização faz com que todas as novas conexões sejam direcionadas para fora do local danificado.

No entanto, clientes com conexões abertas preexistentes podem continuar fazendo solicitações no local danificado até que os clientes se reconectem. Para garantir uma recuperação rápida, recomendamos que você limite a quantidade de tempo que os clientes permanecem conectados aos seus endpoints.

Se você usar um Application Load Balancer, poderá usar a `keepalive` opção para configurar por quanto tempo as conexões continuarão. Para obter mais informações, consulte a duração do keepalive do cliente HTTP no Guia do usuário do Application Load Balancer.

Por padrão, os Application Load Balancers definem o valor da duração do keepalive do cliente HTTP como 3.600 segundos ou 1 hora. Sugerimos que você reduza o valor para estar alinhado com a meta de tempo de recuperação do aplicativo, por exemplo, 300 segundos. Ao escolher o tempo de duração do keepalive de um cliente HTTP, considere que esse valor é uma troca entre se reconectar com mais frequência em geral, o que pode afetar a latência, e afastar mais rapidamente todos os clientes de uma AZ ou região com problemas.

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

Recomendamos que você mantenha uma cópia local dos endpoints do cluster ARC Regional, em marcadores ou salva no código de automação que você usa para tentar novamente seus endpoints. Durante um evento de falha, talvez você não consiga acessar algumas operações de API, incluindo operações de API ARC que não estão hospedadas no cluster de plano de dados extremamente confiável. Você pode listar os endpoints dos seus clusters ARC usando a operação de DescribeClusterAPI.

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

Os controles de roteamento fornecem cinco endpoints regionais para garantir alta disponibilidade, mesmo ao lidar com falhas. Para alcançar sua resiliência total, é importante ter uma lógica de repetição que possa usar todos os cinco endpoints conforme necessário. 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 do plano de dados ARC, visualize seus controles e estados de roteamento com a ListRoutingControlsoperação e atualize os estados de controle de roteamento para redirecionar

o tráfego para failover com a operação. UpdateRoutingControlState Você pode usar o AWS CLI (como nesses exemplos) ou o código que você escreve usando um dos AWS SDKs. O ARC oferece extrema confiabilidade com a API no plano de dados para fazer failover o 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 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.

Teste o failover com o ARC

Teste o failover regularmente com o controle de roteamento ARC, para fazer o failover de sua pilha de aplicativos primária para uma pilha de aplicativos secundária. É importante garantir que as estruturas 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 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.

Operações de API de controle de roteamento

Esta seção inclui tabelas com listas de operações de API que você pode usar para configurar e usar o controle de roteamento no Amazon Application Recovery Controller (ARC), com links para a documentação relevante.

Para obter exemplos de como usar operações comuns da API de configuração de controle de roteamento com o AWS Command Line Interface, consulte Exemplos de uso de operações de API de controle de roteamento ARC com o AWS CLI.

A tabela a seguir lista as operações da API ARC que você pode usar para a configuração do controle de roteamento, com links para a documentação relevante.

Ação	Usando o console ARC	Usando a API ARC
Criar um cluster	Consulte Criação de componentes de controle de roteamento no ARC	Consulte CreateCluster
Descrever um cluster	Consulte Criação de componentes de controle de roteamento no ARC	Consulte DescribeCluster
Excluir um cluster	Consulte Criação de componentes de controle de roteamento no ARC	Consulte DeleteCluster
Listar clusters para uma conta	Consulte Criação de componentes de controle de roteamento no ARC	Consulte ListClusters
Criar um controle de roteamento	Consulte Criação de componentes de controle de roteamento no ARC	Consulte CreateRoutingControl
Descrever um controle de roteamento	Consulte Criação de componentes de controle de roteamento no ARC	Consulte DescribeRoutingControl
Atualizar um controle de roteamento	Consulte Criação de componentes de controle de roteamento no ARC	Consulte UpdateRoutingControl
Excluir um controle de roteamento	Consulte Criação de componentes de controle de roteamento no ARC	Consulte DeleteRoutingControl
Listar os controles de roteamento	Consulte Criação de componentes de controle de roteamento no ARC	Consulte ListRoutingControls

Ação	Usando o console ARC	Usando a API ARC
Criar um novo painel de controle.	Consulte Criação de componentes de controle de roteamento no ARC	Consulte CreateControlPanel
Descrever um painel de controle	Consulte Criação de componentes de controle de roteamento no ARC	Consulte DescribeControlPanel
Atualizar um painel de controle	Consulte Criação de componentes de controle de roteamento no ARC	Consulte UpdateControlPanel
Excluir um painel de controle	Consulte Criação de componentes de controle de roteamento no ARC	Consulte DeleteControlPanel
Listar os painéis de controle	Consulte Criação de componentes de controle de roteamento no ARC	Consulte ListControlPanels
Criar uma regra de segurança	Consulte Criação de regras de segurança para controle de roteamento	Consulte CreateSafetyRule
Descrever uma regra de segurança	Consulte Criação de regras de segurança para controle de roteamento	Consulte DescribeSafetyRule
Atualizar uma regra de segurança	Consulte Criação de regras de segurança para controle de roteamento	Consulte UpdateSafetyRule
Excluir uma regra de segurança	Consulte Criação de regras de segurança para controle de roteamento	Consulte DeleteSafetyRule

Ação	Usando o console ARC	Usando a API ARC
Listar regras de segurança	Consulte Criação de regras de segurança para controle de roteamento	Consulte ListSafetyRules
Listar as verificações de integridade do Route 53 associadas	Consulte Criando uma verificação de integridade do controle de roteamento no ARC	Veja ListAssociatedRoute53HealthChecks
Listar as políticas AWS RAM de recursos para compartilhamento de clusters	Consulte Support cross-account para clusters no ARC	Consulte GetResourcePolicy

A tabela a seguir lista as operações comuns da API ARC que você pode usar para gerenciar o failover de tráfego com o plano de dados de controle de roteamento, com links para a documentação relevante.

Ação	Usando o console ARC	Usando a API ARC
Obter um estado de controle de roteamento	Consulte Obtendo e atualizando estados de controle de roteamento no AWS Management Console	Consulte GetRoutingControlState
Listar os controles de roteamento	N/D	Consulte ListRoutingControls
Atualizar um estado de controle de roteamento	Consulte Obtendo e atualizando estados de controle de roteamento no AWS Management Console	Consulte UpdateRoutingControlState
Atualizar vários estados de controle de roteamento	Consulte Obtendo e atualizando estados de controle	Consulte UpdateRoutingControlStates

Ação	Usando o console ARC	Usando a API ARC
	de roteamento no AWS Management Console	

Usando esse serviço com um AWS SDK

AWS kits de desenvolvimento de software (SDKs) estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que permitem que os desenvolvedores criem facilmente aplicações em seu idioma de preferência.

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

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

Para obter exemplos específicos deste serviço, consulte Exemplos de código para o Application Recovery Controller usando AWS SDKs.

> **Exemplo de disponibilidade**
>
> Não consegue encontrar o que precisa? Solicite um exemplo de código usando o link Fornecer feedback na parte inferior desta página.

Exemplos de uso de operações de API de controle de roteamento ARC com o AWS CLI

Esta seção mostra exemplos simples de aplicações de como trabalhar com controle de roteamento, usando o AWS Command Line Interface para trabalhar com o recurso de controle de roteamento no Amazon Application Recovery Controller (ARC) usando operações de API. Os exemplos têm como objetivo ajudá-lo a desenvolver uma compreensão básica de como trabalhar com o controle de roteamento usando a CLI.

Com o controle de roteamento no Amazon Application Recovery Controller (ARC), você pode acionar failovers de tráfego entre cópias ou réplicas redundantes de aplicativos que estão sendo executadas em zonas separadas ou de disponibilidade. Regiões da AWS

Você organiza os controles de roteamento em grupos chamados painéis de controle que são provisionados em um cluster. Um cluster 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 .

> **Note**
>
> O ARC é um serviço global que oferece suporte a endpoints em vários Regiões da AWS. No entanto, você deve especificar a região Oeste dos EUA (Oregon) — ou seja, especificar o parâmetro `--region us-west-2` — na maioria dos comandos ARC CLI. Por exemplo, use o `region` parâmetro ao criar grupos de recuperação, painéis de controle e clusters. Quando você cria um cluster, o ARC fornece um conjunto de endpoints regionais. Para obter ou atualizar os estados de controle de roteamento, você deve especificar o endpoint regional (o Região da AWS e o URL do endpoint) em seu comando CLI.

Para obter mais informações sobre como usar o AWS CLI, consulte a Referência de AWS CLI Comandos. Para obter uma lista das ações da API de controle de roteamento, consulte Operações de API de controle de roteamento e. Operações de API de controle de roteamento

Começaremos criando os componentes necessários para gerenciar o failover usando controles de roteamento, começando com a criação de um cluster.

Configurar componentes de controle de roteamento

Nossa primeira etapa é criar um cluster. Um cluster ARC é um conjunto de cinco endpoints, um em cada um dos cinco diferentes Regiões da AWS. A infraestrutura ARC permite que esses endpoints trabalhem em coordenação para garantir alta disponibilidade e consistência sequencial das operações de failover.

1. Criar um cluster

1a. Crie um cluster. O `network-type` é opcional e pode ser `IPV4` ou`DUALSTACK`. O padrão é `IPV4`.

```
aws route53-recovery-control-config create-cluster --cluster-name test --network-type
 DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
```

```
}
```

Quando você cria um recurso ARC pela primeira vez, ele tem o status de `PENDING` enquanto o cluster é 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::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

Quando o status é IMPLANTADO, o 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
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

1d. Atualize o tipo de rede dos seus clusters. As opções são `IPV4` ou `DUALSTACK`.

```
aws route53-recovery-control-config update-cluster \
```

```
--cluster-arn arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234 \
--network-type DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
   "NetworkType": "DUALSTACK"
}
```

2. Criar um novo painel de controle.

Um painel de controle é um agrupamento lógico para organizar seus controles de roteamento ARC. Quando você cria um cluster, o 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. Criar 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 um recurso ARC pela primeira vez, 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 recurso 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`.

Criar 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 recursos do 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, você cria regras de segurança de controle de roteamento.

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 para controle de roteamento .

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 AssertionRuleo Guia de referência da API Routing Control para o Amazon Application Recovery Controller.

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 GatingRuleo Guia de referência da API Routing Control para o Amazon Application Recovery Controller.

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 recursos de controle de roteamento, você pode descrever, listar ou excluir regras de segurança depois que elas se propagarem 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
0123456bbbbbbb0123456bbbbbb01234563333333444444
```

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 o tráfego, você cria verificações de saúde no Amazon Route 53 e, em seguida, associa as verificações de saúde aos seus registros de DNS. Para fazer o failover do tráfego, um controle de roteamento ARC define a verificação de integridade como falha, para que o Route 53 redirecione o tráfego. (A verificação de integridade não valida a integridade do seu aplicativo; ela é usada simplesmente como um método para redirecionar o tráfego.)

Por exemplo, digamos que você tenha duas células (regiões ou zonas de disponibilidade). Você configura uma como a célula primária do seu aplicativo e a outra como secundária, para a qual realizar o failover.

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

1. Use o ARC CLI para criar um controle de roteamento para cada célula.
2. Use a CLI do Route 53 para criar uma verificação de integridade do 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**
>
> Você cria verificações de saúde do 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-ffffff22222",
    "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 AWS CLI Comandos do Amazon Route 53 para o change-resource-record-setscomando. 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`.

Liste e atualize os controles e estados de roteamento com o AWS CLI

Depois de criar seus recursos do Amazon Application Recovery Controller (ARC), como cluster, controles de roteamento e painéis de controle, você pode interagir com o cluster para listar e atualizar os estados de controle de roteamento para failover.

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

Você pode usar qualquer um dos endpoints do cluster regional. Recomendamos que seus sistemas passem pelos endpoints regionais e 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 mais informações sobre como usar o AWS CLI, consulte a Referência de AWS CLI Comandos. Para conferir uma lista das ações de API de controle de roteamento e links para mais informações, consulte Operações de API de 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 o AWS CLI ou um AWS SDK. O ARC oferece extrema confiabilidade com o plano de dados de controle de roteamento ARC para redirecionar o tráfego e fazer o failover entre as células. Para obter mais recomendações sobre o uso do ARC para failover, consulteMelhores práticas para controle de roteamento no ARC.

Ao criar 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 um `ClusterEndpoint` inclui uma região

e um endpoint correspondente que você pode usar para obter ou atualizar os estados de controle de roteamento. DescribeClusteré uma operação de API de configuração de controle de recuperação. Recomendamos que você mantenha uma cópia local dos endpoints do cluster ARC Regional, em marcadores ou codificada no código de automação que você usa para tentar novamente seus endpoints.

1. Listar os controles de roteamento

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

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. Obtenha controles de roteamento

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"
}
```

2. Atualizar controles de roteamento

Para rotear o tráfego para o endpoint de destino controlado pelo controle de roteamento, atualize o estado do controle de roteamento para 0n. 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
```

```
{}
```

Trabalhando com componentes de controle de roteamento no ARC

Tópicos

- Criação de componentes de controle de roteamento no ARC
- Visualizando e atualizando estados de controle de roteamento no ARC
- Criação de regras de segurança para controle de roteamento
- Support cross-account para clusters no ARC

Criação de componentes de controle de roteamento no ARC

Esta seção explica como criar um cluster, controles de roteamento, verificações de saúde e painéis de controle para trabalhar com o controle de roteamento no Amazon Application Recovery Controller (ARC).

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 a réplica de backup, por exemplo.

Observe que você será cobrado por hora para cada cluster que criar. 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 recursos usando AWS Resource Access Manager, para que um cluster possa hospedar controles de roteamento e outros recursos ARC pertencentes a vários Contas da AWS. Para saber mais sobre o compartilhamento de recursos no ARC, Support cross-account para clusters no ARC. Para obter informações sobre preços, consulte os preços do Amazon Application Recovery Controller (ARC) e desça 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 obter mais informações, consulte Criação de regras de segurança para controle de roteamento .

As etapas para criar os componentes para controle de roteamento no console ARC estão incluídas nessas seções. Para saber mais sobre como usar as operações da API de configuração de controle de recuperação com o ARC, consulte Operações de API de controle de roteamento o.

Criando um cluster no ARC

Você deve criar um cluster para hospedar controles de roteamento e painéis de controle no 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 emhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Escolha Clusters.
3. Escolha Criar e insira um nome para o cluster.
4. Selecione Criar cluster.

Criando um controle de roteamento no 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 recursos que você separou para fins de recuperação, você pode ter uma célula para cada um e células aninhadas para cada Região da AWS 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 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.

Criando uma verificação de integridade do controle de roteamento no 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 Amazon Application Recovery Controller (ARC) simplesmente atualizando o estado do controle de roteamento associado, para configurá-lo como ou. `On` `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 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 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 ARC (recomendado).

Para ver exemplos dos AWS CLI comandos para criar controles de roteamento e as verificações de integridade associadas usando as operações da API ARC, consulte Exemplos de uso de operações de API de controle de roteamento ARC com o AWS CLI.

Criando um painel de controle no ARC

Um painel de controle no Amazon Application Recovery Controller (ARC) 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.

Quando você cria um cluster, o 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 ARC estão incluídas nesta seção. Para obter informações sobre como usar as operações da API de configuração de controle de recuperação com o ARC, consulte Operações de API de controle de roteamento o.

Como criar um painel de controle

1. Abra o console ARC 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.

Visualizando e atualizando estados de controle de roteamento no ARC

Esta seção descreve como visualizar e atualizar os estados de controle de roteamento no Amazon Application Recovery Controller (ARC). Os controles de roteamento são simples interruptores liga-desliga que gerenciam o fluxo de tráfego para as células do seu grupo de recuperação. Normalmente Regiões da AWS, as células são, ou às vezes, zonas de disponibilidade, que incluem seus recursos. Quando um estado de controle de roteamento é 0n, 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 ARC ou usando a API ARC. Recomendamos atualizar os estados de controle de roteamento usando a API. Primeiro, o 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 `0ff` 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 ARC (recomendado)

Recomendamos que você use as operações de API do Amazon Application Recovery Controller (ARC) para obter ou atualizar estados de controle de roteamento, usando um AWS CLI comando ou código que você desenvolveu para usar operações de API 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 ARC oferece extrema confiabilidade para o failover entre células (Regiões da AWS) ao atualizar os estados de controle de roteamento usando a API, pois os controles de roteamento são armazenados em um cluster altamente disponível. O ARC garante que pelo menos três dos cinco endpoints regionais do cluster estejam sempre acessíveis para você fazer 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 da API ARC para 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 o AWS CLI para obter e atualizar estados de controle de roteamento, consulte Liste e atualize os controles e estados de roteamento com o AWS CLI.

Obtendo e atualizando 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 Amazon Application Recovery Controller (ARC). Além disso, o console não está altamente disponível, enquanto o plano de dados ARC oferece extrema confiabilidade. Por esses motivos, recomendamos que você use a API ARC para obter e atualizar os estados de controle de roteamento para operações de produção.

Para obter mais recomendações sobre o uso do ARC para failover, consulteMelhores práticas para controle de roteamento no ARC.

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 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/casa.

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 para controle de roteamento

Ao trabalhar com vários controles de roteamento ao mesmo tempo, você pode decidir que deseja implementar salvaguardas para evitar consequências não intencionais. 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 ARC, você cria regras de segurança.

Você configura as regras de segurança para controle de roteamento 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 ARC impõe que os critérios definidos ao configurar a regra sejam atendidos, ou então os estados de controle de roteamento não sejam 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 AWS CLI comando que cria uma regra de afirmação para impor esses critérios, consulte Criar regras de segurança em. Exemplos de uso de operações de API de controle de roteamento ARC com o 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 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 AWS CLI comando que cria uma regra de controle que implementa esse tipo de opção geral, consulte Criar regras de segurança em. Exemplos de uso de operações de API de controle de roteamento ARC com o 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 Application Recovery Controller.

Criar uma regra de segurança no console

As etapas desta seção explicam como criar uma regra de segurança no console 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 Amazon Application Recovery Controller (ARC), consulte Operações de API de controle de roteamento.

Como criar uma regra de segurança

1. Abra o console ARC 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 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 Application Recovery Controller.

8. Escolha Criar.

Editar ou excluir uma regra de segurança no console

As etapas desta seção explicam como editar ou excluir uma regra de segurança no console ARC. Você só pode fazer edições limitadas em uma regra de segurança para alterar o nome ou atualizar o período de espera. Para fazer outras alterações, exclua e recrie a regra de segurança.

Para saber mais sobre o uso de operações de API com o Amazon Application Recovery Controller (ARC), consulte Operações de API de controle de roteamento o.

Como excluir uma regra de segurança

1. Abra o console ARC 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 ignorar as regras de segurança ao atualizar um estado de controle de roteamento (ou vários estados de controle de roteamento) usando o `update-routing-control-states` AWS CLI comando `update-routing-control-state` ou com o parâmetro. `safety-rules-to-override` Especifique o parâmetro com o Amazon Resource Name (ARN) da regra de segurança que você deseja substituir ou especifique uma lista separada por vírgulas ARNs para substituir 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 a regra de segurança ARNs à lista de regras a serem substituídas no comando de atualização, separadas 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 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
```

Support cross-account para clusters no ARC

O Amazon Application Recovery Controller (ARC) 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 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 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. 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 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 ARC, especialmente se você tiver um grande número de aplicativos distribuídos em várias contas e equipes operacionais.

Para começar com o compartilhamento entre contas no ARC, você cria 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 o AWS Management Console ou executando operações da API ARC usando o AWS Command Line Interface ou AWS SDKs.

Este tópico explica como compartilhar recursos que você possui e como usar os recursos que são compartilhados com você.

Conteúdo

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 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 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 o AWS Command Line Interface ou AWS SDKs.

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 o AWS CLI ou SDKs.

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.

Concedendo permissões para compartilhar clusters

O compartilhamento de clusters entre contas requer permissões para que o principal do IAM compartilhe o cluster por meio de AWS RAM.

Recomendamos usar a política `AmazonRoute53RecoveryControlConfigFullAccess` gerenciada do IAM para garantir que seus diretores do IAM tenham as permissões necessárias para compartilhar e usar clusters compartilhados.

Compartilhar um cluster usando uma política personalizada do IAM exige `route53-recovery-control-config:PutResourcePolicyroute53-recovery-control-config:GetResourcePolicy`,, e `route53-recovery-control-config:DeleteResourcePolicy` permissões para esse cluster. `PutResourcePolicye DeleteResourcePolicy` são ações do IAM somente com permissão. Tentar compartilhar um cluster AWS RAM sem ter essas permissões resultará em um erro.

Para obter mais informações sobre a forma como AWS Resource Access Manager usa o IAM, consulte Como AWS Resource Access Manager usa o IAM no Guia AWS RAM do usuário.

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 o AWS CLI ou SDKs.

Para cancelar o compartilhamento de um cluster compartilhado que você possui usando o console AWS RAM

Consulte Atualização de um compartilhamento de recursos no Guia 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 ARC AWS CLI e.

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 AWS Command Line Interface operações da API ARC.

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, usando o AWS Command Line Interface ou. AWS SDKs

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 integridade 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 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 Amazon Application Recovery Controller (ARC) e role para baixo até Amazon Application Recovery Controller (ARC).

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. Se as contas que compartilham o recurso do cluster tiverem uma cota maior do que as cotas do proprietário do cluster, as cotas do proprietário do cluster terão precedência sobre as cotas das contas que estão compartilhando.

Para entender melhor como isso funciona, veja os exemplos a seguir. Para ilustrar como as cotas funcionam com o compartilhamento de recursos, para esses exemplos, digamos que o proprietário do cluster seja Proprietário e uma conta com a qual o cluster foi compartilhado seja Participante.

Cota de painéis de controle

As cotas são impostas para o total de painéis de controle do proprietário por cluster.

Por exemplo, digamos que o proprietário tenha uma cota de 50 para o número de painéis de controle por cluster e tenha 13 painéis de controle no cluster. Agora, digamos que o Participante tenha a cota definida como 150. Nesse cenário, o Participante só pode criar até 37 painéis de controle (ou seja, 50-13) no cluster compartilhado.

Além disso, se outras contas que compartilham o cluster também criarem painéis de controle, todas elas também contam para a cota geral do cluster de 50 painéis de controle.

Cotas de controle de roteamento

Os controles de roteamento têm várias cotas: uma cota por painel de controle, uma cota por cluster e uma cota por regra de segurança. As cotas do proprietário têm precedência para todas essas cotas.

Por exemplo, digamos que o proprietário tenha uma cota de 300 para o número de controles de roteamento por cluster e já tenha 300 controles de roteamento no cluster. Agora, digamos que

o Participante tenha essa cota definida como 500. Nesse cenário, o Participante não pode criar novos controles de roteamento no cluster compartilhado.

Regras de segurança e cotas

As cotas são aplicadas de acordo com as regras de segurança do proprietário por cota do painel de controle.

Por exemplo, digamos que o Proprietário tenha uma cota de 20 para o número de regras de segurança por painel de controle e o Participante tenha essa cota definida como 80. Nesse cenário, como o limite inferior do proprietário tem precedência, o participante só pode criar até 20 regras de segurança em um painel de controle no cluster compartilhado.

Para obter uma lista de cotas de controle de roteamento, consulte. Cotas para controle de roteamento

Registro e monitoramento para controle de roteamento no Amazon Application Recovery Controller (ARC)

Você pode usar AWS CloudTrail para monitorar o controle de roteamento no Amazon Application Recovery Controller (ARC), para analisar padrões e ajudar a solucionar problemas.

Tópicos

- Registrando chamadas da API ARC usando AWS CloudTrail

Registrando chamadas da API ARC usando AWS CloudTrail

é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no ARC. CloudTrail captura todas as chamadas de API para ARC como eventos. As chamadas capturadas incluem chamadas do console ARC e chamadas de código para as operações da API ARC.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para 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 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 sobre ARC em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no ARC, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do 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 eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do ARC são registradas CloudTrail e documentadas no Guia de referência da API Recovery Readiness para o Amazon Application Recovery Controller, no Guia de referência da API de configuração de controle de recuperação para o Amazon Application Recovery Controller e no Guia de referência da API Routing Control para o Amazon 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 o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Visualizando eventos ARC no histórico de eventos

CloudTrail permite que você visualize eventos recentes no histórico de eventos. Para visualizar eventos para solicitações da API 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.

Entendendo as entradas do arquivo de log 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 configurar o controle de roteamento.

```
{
  "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"
```

```
}
```

Identity and Access Management para controle de roteamento

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 (conectado) e autorizado (tem permissões) para usar os recursos do ARC. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Conteúdo

Como o controle de roteamento no Amazon Application Recovery Controller (ARC) funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao controle de roteamento no Amazon Application Recovery Controller (ARC), saiba quais recursos do IAM estão disponíveis para uso com o controle de roteamento.

Recursos do IAM que você pode usar com controle de roteamento no Amazon Application Recovery Controller (ARC)

Atributo do IAM	Suporte ao controle de roteamento
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim

Atributo do IAM	Suporte ao controle de roteamento
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para obter uma visão geral de alto nível de como os AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS Serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para ARC

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 do IAM, grupo de usuários ou perfil. 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 Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim 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 perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Para ver exemplos de políticas baseadas em identidade ARC para controle de roteamento, consulte. Exemplos de políticas baseadas em identidade para controle de roteamento no Amazon Application Recovery Controller (ARC)

Políticas baseadas em recursos dentro do controle de roteamento

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos 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 políticas para controle de roteamento

Compatível com 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 podem ser usadas 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. Algumas operações também 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 de ações do ARC para controle de roteamento, consulte Ações definidas pelos controles de recuperação do Amazon Route 53 e Ações definidas pelo cluster de recuperação do Amazon Route 53 na Referência de autorização de serviço.

As ações de política no ARC para controle de roteamento usam os seguintes prefixos antes da ação, dependendo da API com a qual você está trabalhando:

```
route53-recovery-control-config
route53-recovery-cluster
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas. Por exemplo, você pode fazer o seguinte:

```
"Action": [
      "route53-recovery-control-config:action1",
      "route53-recovery-control-config: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-control-config:Describe*"
```

Para ver exemplos de políticas baseadas em identidade ARC para controle de roteamento, consulte. Exemplos de políticas baseadas em identidade para controle de roteamento no Amazon Application Recovery Controller (ARC)

Recursos políticos para ARC

Compatível com 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 de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Na Referência de Autorização de Serviço, você pode ver as seguintes informações relacionadas ao ARC:

Para ver uma lista dos tipos de recursos e seus ARNs, e as ações que você pode especificar com o ARN de cada recurso, consulte os tópicos a seguir na Referência de Autorização de Serviço:

- Ações definidas pelos controles de recuperação do Amazon Route 53
- Ações definidas pelo Amazon Route 53 Recovery Cluster.

Para ver exemplos de políticas baseadas em identidade ARC para controle de roteamento, consulte. Exemplos de políticas baseadas em identidade para controle de roteamento no Amazon Application Recovery Controller (ARC)

Chaves de condição de política para ARC

Compatível com chaves de condição de política específicas de 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 `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `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 antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar 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 da 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 das chaves de condição ARC para controle de roteamento, consulte os tópicos a seguir na Referência de Autorização de Serviço:

- Chaves de condição para os controles de recuperação do Amazon Route 53
- Chaves de condição para o cluster de recuperação 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:

- Para ver uma lista dos tipos de recursos e seus ARNs, consulte Ações definidas pelos controles de recuperação do Amazon Route 53 e Ações definidas pelo cluster de recuperação do Amazon Route 53.

- Para ver uma lista das ações que você pode especificar com o ARN de cada recurso, consulte Recursos definidos pelos controles de recuperação do Amazon Route 53 e Recursos definidos pelo cluster de recuperação do Amazon Route 53.

Para ver exemplos de políticas baseadas em identidade ARC para controle de roteamento, consulte Exemplos de políticas baseadas em identidade para controle de roteamento no Amazon Application Recovery Controller (ARC)

Listas de controle de acesso (ACLs) em ARC

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso baseado em atributos (ABAC) com ARC

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as 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. Marcar de entidades e atributos 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 estiver 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 chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do 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 controle de roteamento ARC inclui o seguinte suporte para ABAC:

- O Recovery Control Config é compatível com ABAC.
- O cluster de recuperação não oferece suporte ao ABAC.

Usando credenciais temporárias com o ARC

Compatível com 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 funções, consulte Alternar para um perfil do IAM (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 principais entre serviços para ARC

Compatibilidade com o recurso de 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. Permissões concedidas por políticas a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, acionar 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

Funções de serviço para ARC

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar 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.

Funções vinculadas a serviços para ARC

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS serviço. O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua AWS conta e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

O controle de roteamento não usa funções vinculadas ao serviço.

Exemplos de políticas baseadas em identidade para controle de roteamento no Amazon Application Recovery Controller (ARC)

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do ARC. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos 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 aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo ARC, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon Application Recovery Controller (ARC) na Referência de autorização de serviço. ARNs

Tópicos

- Práticas recomendadas de política
- Exemplo: acesso ao console ARC para controle de roteamento

- Exemplos: ações da API ARC para configuração de controle de roteamento

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos ARC em sua conta. Essas ações podem incorrer em custos para sua 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 funções 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 da 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 cem verificações de política e recomendações práticas para ajudar 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 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 ARC para controle de roteamento

Para acessar o console do Amazon Application Recovery Controller (ARC), você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do ARC em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva 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 à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do ARC quando você permite acesso somente a operações específicas da API, anexe também uma política `ReadOnly` AWS gerenciada para o ARC às entidades. Para obter mais informações, consulte a página de políticas gerenciadas do ARC ARC ou Adicionar permissões a um usuário no Guia do usuário do IAM.

Para dar aos usuários acesso total ao uso dos recursos de controle de roteamento ARC por meio do console, anexe uma política como a seguinte ao usuário, para dar ao usuário permissões completas para configurar recursos e operações de controle de roteamento 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: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"
            ],
            "Resource": "*"
        },
                {
            "Effect": "Allow",
            "Action": [
                "route53:GetHealthCheck",
                "route53:CreateHealthCheck",
                "route53:DeleteHealthCheck",
                "route53:ChangeTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplos: ações da API ARC para configuração de controle de roteamento

Para garantir que um usuário possa usar as ações da API ARC para trabalhar com a configuração do controle de roteamento ARC, anexe uma política que corresponda às operações da API com as quais o usuário precisa trabalhar, conforme descrito abaixo.

Para trabalhar com operações de API para configuração 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:GetResourcePolicy",
                   "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": "*"
        }
    ]
}
```

Para realizar tarefas no controle de roteamento do ARC com a API do plano de dados do cluster de recuperação, por exemplo, atualizando os estados do controle de roteamento para o failover durante um evento de desastre, você pode anexar uma política do ARC IAM, 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 obter 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 a substituição das regras de segurança, você pode anexar uma política como a seguinte, com `AllowSafetyRuleOverrides` boolean a. `false` Para permitir que o operador anule as regras de segurança, defina o `AllowSafetyRuleOverrides` booleano como. `true`

```
{
    "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": "false"
                }
            }
        }
    ]
}
```

AWS políticas gerenciadas para controle de roteamento no Amazon Application Recovery Controller (ARC)

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 elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são 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) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

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 do controle de recuperação no 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. Essa política concede acesso somente de leitura às ações para trabalhar com

a configuração do controle de recuperação no 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 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. Essa política concede acesso somente de leitura ao plano de dados do cluster no 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 para políticas AWS gerenciadas para controle de roteamento

Para obter detalhes sobre as atualizações das políticas AWS gerenciadas para controle de roteamento no ARC desde que esse serviço começou a rastrear essas alterações, consulteAtualizações nas políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC). Para alertas automáticos sobre alterações nesta página, assine o feed RSS na página de histórico do documento ARC.

Cotas para controle de roteamento

O controle de roteamento no Amazon Application Recovery Controller (ARC) está sujeito às seguintes cotas (anteriormente chamadas de limites).

Entidade	Quota

Entidade	Quota
Número de clusters por conta	2
Número de painéis de controle por cluster	50
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 UpdateRoutingControlStatesoperação	10
Número de chamadas de API de mudança para um endpoint de cluster, por segundo	3

Verificação de prontidão no ARC

Com a verificação de prontidão no Amazon Application Recovery Controller (ARC), você pode obter informações sobre se seus aplicativos e recursos estão preparados para recuperação. Depois de modelar seu AWS aplicativo no ARC e criar verificações de prontidão, as verificações monitoram continuamente as informações sobre seu aplicativo, como cotas de AWS recursos, capacidade e políticas de roteamento de rede. Em seguida, você pode optar por ser notificado sobre alterações que afetariam sua capacidade de fazer o failover em uma réplica do seu aplicativo para se recuperar de um evento. As verificações de prontidão ajudam a garantir, de forma contínua, que você possa manter seus aplicativos multirregionais em um estado dimensionado e configurado para lidar com o tráfego de failover.

Este capítulo explica como modelar seu aplicativo no ARC para configurar a estrutura que permite que as verificações de prontidão funcionem, criando um grupo de recuperação e células que descrevam seu aplicativo. Em seguida, você pode seguir as etapas para adicionar verificações de prontidão e escopos de prontidão para que o ARC possa auditar a prontidão do seu aplicativo.

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

O que é verificação de prontidão no Amazon Application Recovery Controller (ARC)?

Uma verificação de prontidão no ARC audita continuamente (em intervalos de um minuto) as incompatibilidades na capacidade AWS provisionada, cotas de serviço, limites de aceleração e 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 do Auto Scaling com capacidade de buffer suficiente em cada réplica para gerenciar se outra célula não estiver disponível.

Para cotas, quando o 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 que possa 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 ()). AZs

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. Existem conjuntos de regras de prontidão para cada tipo de recurso, que as verificações do 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 AWS Management Console, no ou usando ações da API ARC. 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 ARC para facilitar a configuração e o monitoramento de recursos distribuídos a partir de uma única AWS conta.

Monitoramento de réplicas de aplicativos com verificações de prontidão

O ARC audita suas réplicas de aplicativos usando verificações de prontidão para garantir que cada uma tenha a mesma configuração e o mesmo estado de tempo de execução. Uma verificação de prontidão audita continuamente a capacidade AWS dos recursos, a configuração, as AWS cotas e as políticas de roteamento de um aplicativo, informações que você pode usar para ajudar a garantir que as réplicas estejam prontas para o failover. As verificações de prontidão ajudam você a garantir que seu ambiente de recuperação seja dimensionado e configurado para realizar failover quando necessário.

As seções a seguir fornecem mais detalhes sobre como a verificação de prontidão funciona.

Verificações de prontidão e réplicas de seus aplicativos

Para estar preparado para a recuperação, você deve manter capacidade ociosa suficiente em réplicas em todos os momentos, para absorver o tráfego de failover de outra zona ou região de disponibilidade. O ARC inspeciona continuamente (uma vez por minuto) seu aplicativo para garantir que sua capacidade provisionada corresponda a todas as zonas ou regiões de disponibilidade.

A capacidade que o ARC inspeciona inclui, por exemplo, contagens de EC2 instâncias da Amazon, 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 também de aumentar os valores correspondentes em sua réplica em espera, o ARC detectará a incompatibilidade para que você possa aumentar os valores na réplica em espera.

> **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.

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 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 obter mais informações, consulte Usando a verificação de prontidão no 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 obter mais informações, consulte Operações de API de verificação de prontidão.

Como funciona a verificação de prontidão

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

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 ARC inspeciona continuamente (uma vez por minuto) seu aplicativo para garantir que sua capacidade provisionada corresponda a todas as zonas ou regiões de disponibilidade. A capacidade que o ARC inspeciona inclui, por exemplo, contagens de EC2 instâncias da Amazon, 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 também de aumentar os valores correspondentes em sua réplica em espera, o ARC detectará a incompatibilidade para que você possa aumentar os valores na réplica em espera.

> **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.

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 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 obter mais informações, consulte Usando a verificação de prontidão no 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 obter mais informações, consulte Operações de API de verificação de prontidão.

Como as regras de prontidão determinam o estado

As verificações de prontidão do 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 ARC inclui um grupo de regras para cada tipo de recurso que ele suporta. Por exemplo, o ARC tem grupos de regras de prontidão para clusters Amazon Aurora, grupos de 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 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 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 de recursos ou ver um resumo do status de prontidão para um grupo de recuperação ou uma célula (ou seja, uma AWS região 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 `ACTIVE` estado.

- 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 tudo VPC sub-redes para garantir que tenham o mesmo número de sub-redes.
- 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 ele esteja conectado somente a uma zona de disponibilidade. Nota: essa regra não afeta o status de prontidão.

Além disso, o ARC dá um passo extra para as 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 ARC aumenta 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.

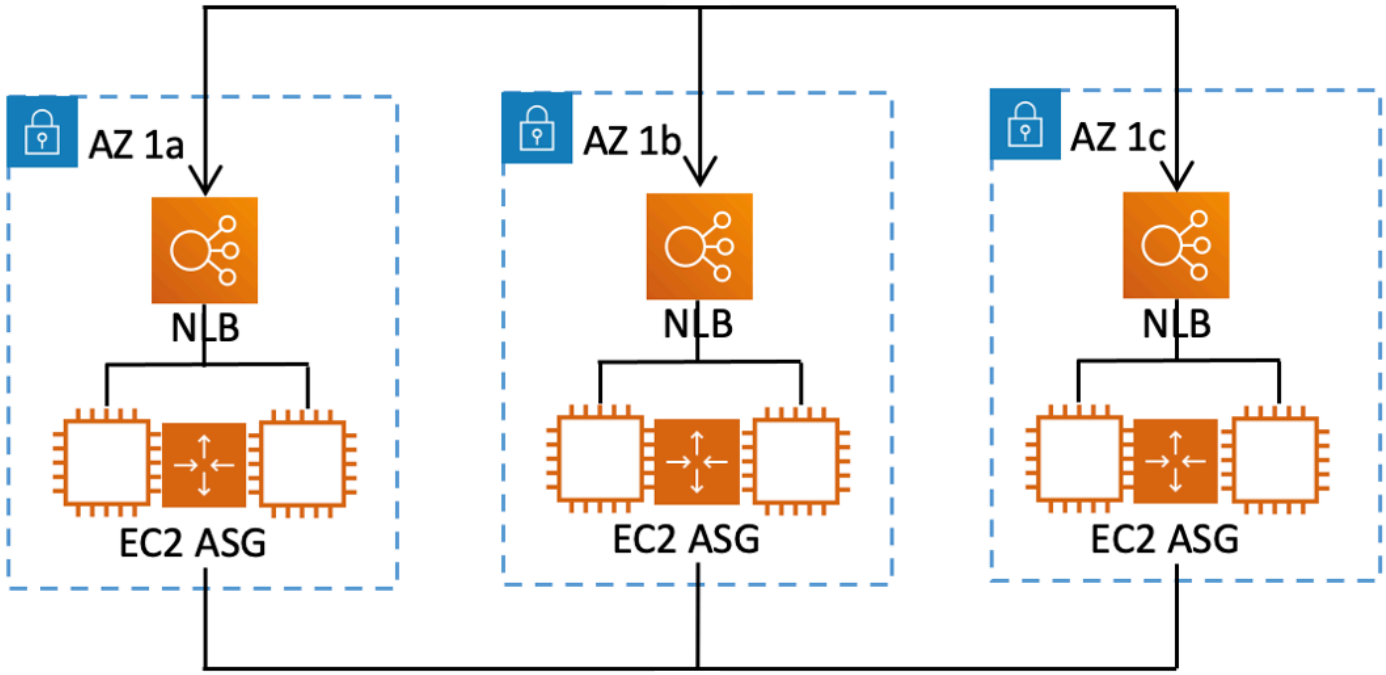
Você também pode configurar uma EventBridge notificação da Amazon para verificações de prontidão, por exemplo, quando o status de qualquer verificação de prontidão mudar para. `NOT READY` Então, quando uma incompatibilidade de configuração é detectada, EventBridge você recebe uma notificação e você pode tomar medidas corretivas para garantir que as réplicas do aplicativo estejam alinhadas e preparadas para recuperação. Para obter mais informações, consulte Usando a verificação de prontidão no ARC com a Amazon EventBridge.

Como as verificações de prontidão, os conjuntos de recursos e os escopos de prontidão funcionam juntos

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 que estão nas células (zonas de disponibilidade ou AWS regiões) em seu grupo de recuperação ARC, para que você possa 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 ARC mostre o status correto `READY` ou de prontidão para verificações resumidas de `NOT READY` prontidão do grupo de recuperação e verificações resumidas de prontidão em nível de célula. A menos que você defina escopos de prontidão, o 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).

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 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 que estão agrupadas em zonas ou AWS regiões de disponibilidade, de forma que as réplicas possam falhar independentemente umas das outras. Se seu aplicativo precisar ser ajustado para ser colocado em silos corretamente, o ARC sugerirá alterações que você pode fazer, se necessário, para atualizar sua arquitetura para ajudar a garantir que ela seja resiliente e pronta para o failover.

O 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 isoladas por zona de disponibilidade ou por região. Em seguida, o ARC identifica e fornece informações sobre os recursos do aplicativo nas células, para determinar se eles 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 obter mais informações, consulte Obtendo recomendações de arquitetura no ARC.

Verificações de prontidão e cenários de recuperação de desastres

As verificações de prontidão do ARC fornecem informações sobre se seus aplicativos e recursos estão prontos para recuperação, ajudando você a garantir que seus aplicativos sejam dimensionados 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`.

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

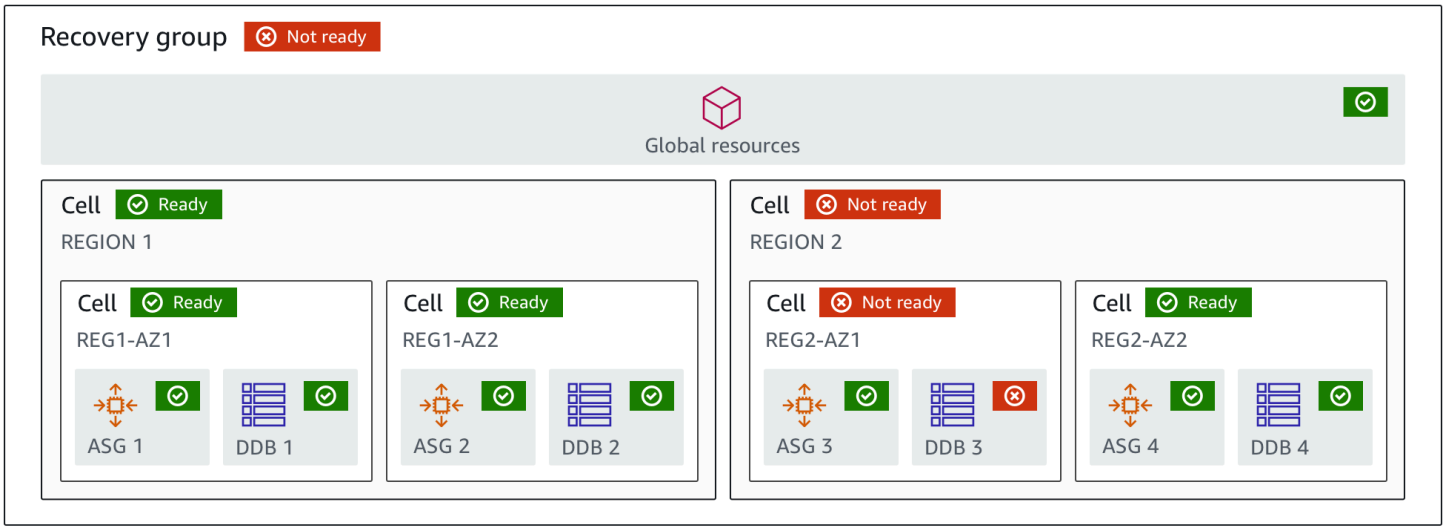
AWS Disponibilidade da região para verificação de prontidão

Para obter informações detalhadas sobre endpoints regionais de suporte e serviço para o Amazon Application Recovery Controller (ARC), consulte os endpoints e cotas do Amazon Application Recovery Controller (ARC) na Referência geral da Amazon Web Services.

> **Note**
>
> A verificação de prontidão no Amazon Application Recovery Controller (ARC) é um recurso global. No entanto, os recursos de verificação de prontidão estão na região Oeste dos EUA (Oregon), portanto, você deve especificar a região Oeste dos EUA (Oregon) (especifique o parâmetro`--region us-west-2`) nos AWS CLI comandos regionais do ARC, por exemplo, ao criar recursos como conjuntos de recursos e verificações de prontidão.

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 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 (células aninhadas) dentro de uma célula, como AZs dentro de 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 web replicado em us-east-1a e us-east-1b, em que us-east-1b é seu ambiente de failover, você pode representar esse aplicativo no 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 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 de recurso. Um identificador de recurso é o Amazon Resource Name (ARN) do recurso ou, para um recurso de destino de DNS, o identificador que o ARC gera ao criar o recurso.

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 ARC para recursos de destino de DNS e, em seguida, criar uma verificação de prontidão para o conjunto de recursos para que você possa 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 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 ARC realiza em relação a um conjunto de recursos em um conjunto de recursos. O ARC tem um conjunto de regras de prontidão para cada tipo de recurso para o qual ele suporta verificações de prontidão. Cada regra inclui um ID e uma descrição que explicam para que o ARC inspeciona os recursos.

Verificação de prontidão

Uma verificação de prontidão monitora um conjunto de recursos em seu aplicativo, como um conjunto de instâncias do Amazon Aurora, para o qual o ARC está auditando a 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 recursos, um para cada grupo do Auto Scaling. Em seguida, para garantir que cada grupo seja escalado igualmente, o 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 que seja um recurso global para o ARC, defina o escopo de prontidão no nível do grupo de recuperação ou do recurso global. Por exemplo, uma verificação de saúde do Route 53 é um recurso global no ARC porque não é específica para uma região ou zona de disponibilidade.

Planos de dados e controle para verificação de prontidão

Ao planejar o failover e a recuperação de desastres, considere a resiliência de seus mecanismos de failover. Recomendamos que você certifique-se de que os mecanismos dos quais você depende durante o failover estejam altamente disponíveis, para que você possa usá-los quando precisar deles em um cenário de desastre. Normalmente, você deve usar funções de plano de dados para seus mecanismos sempre que possível, 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 ambientes de gerenciamento e planos de dados e quando você pode confiar em uma expectativa de extrema confiabilidade com o plano de dados de um serviço.

Como acontece com a maioria dos AWS serviços, a funcionalidade do recurso de verificação de prontidão é suportada por planos de controle e planos de dados. Embora ambos tenham sido criados para serem confiáveis, um plano de controle é otimizado para consistência de dados, enquanto um plano de dados é otimizado para disponibilidade. Um plano de dados é projetado para ser resistente e manter a disponibilidade mesmo durante eventos de ruptura, quando um ambiente de gerenciamento pode ficar indisponível.

Em geral, um ambiente de gerenciamento 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 verificar a prontidão, há uma única API, a Recovery Readiness API, 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 de verificação de prontidão e o plano de dados são confiáveis, mas não estão altamente disponíveis.

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.

Marcação para verificação de prontidão no Amazon Application Recovery Controller (ARC)

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 na verificação de prontidão no ARC:

- Conjuntos de recursos
- Verificação de prontidão

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

A seguir estão exemplos de marcação na verificação de prontidão usando o. AWS CLI

```
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
```

Para obter mais informações, consulte TagResourceo Guia de referência da API Recovery Readiness para o Amazon Application Recovery Controller (ARC).

Preços para verificação de prontidão no ARC

Você paga um custo por hora por verificação de prontidão configurada.

Para obter informações detalhadas sobre preços do ARC e exemplos de preços, consulte Preços do ARC.

Configure um processo de recuperação resiliente para seu aplicativo

Para usar o Amazon Application Recovery Controller (ARC) com AWS aplicativos que estão em várias AWS regiões, há diretrizes a serem seguidas para configurar seus aplicativos para resiliência, para que você possa apoiar a prontidão de recuperação de forma eficaz. 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 ARC fornece sobre a arquitetura do seu aplicativo que pode melhorar a resiliência.

> **Note**
>
> Se você tiver um aplicativo isolado por zonas de disponibilidade, considere usar o deslocamento zonal ou o deslocamento automático zonal para recuperação de failover. Nenhuma configuração é necessária para usar o deslocamento zonal ou o deslocamento automático zonal para recuperar de forma confiável os aplicativos das deficiências da Zona de Disponibilidade.
> Para afastar o tráfego de uma zona de disponibilidade para recursos do balanceador de carga, inicie uma mudança zonal no console do ARC ou no console do Elastic Load Balancing. Ou você pode usar o AWS SDK AWS Command Line Interface ou com ações da API de mudança zonal. Para obter mais informações, consulte Mudança zonal no ARC.

Para saber mais sobre como começar a usar configurações de failover resilientes, consulte. Introdução à recuperação multirregional no Amazon Application Recovery Controller (ARC)

Melhores práticas para verificação de prontidão no ARC

Recomendamos as seguintes melhores práticas para verificação de prontidão no Amazon Application Recovery Controller (ARC).

Adicione notificações para alterações no status de prontidão

Defina uma regra na 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 EventBridge regras para enviar notificações para várias alterações no status da verificação de prontidão, inclusive para seu grupo de recuperação (para seu aplicativo), para uma célula (como uma AWS região) ou para uma verificação de prontidão para um conjunto de recursos.

Para obter mais informações, consulte Usando a verificação de prontidão no ARC com a Amazon EventBridge.

Operações de API de verificação de prontidão

A tabela a seguir lista as operações ARC que você pode usar para preparação de 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 Exemplos de uso de operações de API de verificação de prontidão do ARC com o AWS CLI.

Ação	Usando o console ARC	Usando a API ARC
Criar uma célula	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte CreateCell
Obter uma célula	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte GetCell

Ação	Usando o console ARC	Usando a API ARC
Excluir uma célula	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte DeleteCell
Atualizar uma célula	N/D	Consulte UpdateCell
Listar células para uma conta	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte ListCells
Criar um grupo de recuperação	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte CreateRecoveryGroup
Obter um grupo de recuperação	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte GetRecoveryGroup
Atualizar um grupo de recuperação	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte UpdateRecoveryGroup
Excluir o grupo de recuperação	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte DeleteRecoveryGroup
Listar grupos de recuperação	Consulte Criando, atualizando e excluindo grupos de recuperação no ARC	Consulte ListRecoveryGroups
Criar um conjunto de recursos.	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte CreateResourceSet
Obter um conjunto de recursos	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte GetResourceSet

Ação	Usando o console ARC	Usando a API ARC
Atualizar um conjunto de recursos	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte UpdateResourceSet
Excluir um conjunto de recursos	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte DeleteResourceSet
Listar conjuntos de recursos	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte ListResourceSets
Criar uma verificação de prontidão	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte CreateReadinessCheck
Obter uma verificação de prontidão	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte GetReadinessCheck
Atualizar uma verificação de prontidão	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte UpdateReadinessCheck
Excluir uma verificação de prontidão	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte DeleteReadinessCheck
Listar verificações de prontidão	Consulte Criando e atualizando verificações de prontidão no ARC	Consulte ListReadinessChecks
Listar regras de prontidão	Consulte Descrições das regras de prontidão no ARC	Consulte ListRules

Ação	Usando o console ARC	Usando a API ARC
Obter o status de uma verificação de prontidão completa	Consulte Monitorando o status de prontidão no ARC	Consulte GetReadinessCheckStatus
Verificar o status de um recurso	Consulte Monitorando o status de prontidão no ARC	Consulte GetReadinessCheckResourceStatus
Verificar o status de uma célula	Consulte Monitorando o status de prontidão no ARC	Consulte GetCellReadinessSummary
Verificar o status de um grupo de recuperação	Consulte Monitorando o status de prontidão no ARC	Consulte GetRecoveryGroupReadinessSummary

Exemplos de uso de operações de API de verificação de prontidão do ARC com o AWS CLI

Esta seção mostra exemplos simples de aplicativos, usando os recursos de verificação de prontidão AWS Command Line Interface para trabalhar com os recursos de verificação de prontidão no Amazon Application Recovery Controller (ARC) usando operações de API. Os exemplos têm como objetivo ajudá-lo a desenvolver uma compreensão básica de como trabalhar com recursos de verificação de prontidão usando a CLI.

Verificação de prontidão nas auditorias do ARC quanto a incompatibilidades dos recursos em suas réplicas de aplicativos. Para configurar verificações de prontidão para seu aplicativo, você deve configurar — ou modelar — seus recursos de aplicativo em células ARC que se alinhem às réplicas que você criou para seu aplicativo. Em seguida, você configura verificações de prontidão que auditam essas réplicas, para ajudá-lo a garantir que a réplica do aplicativo em espera e seus recursos correspondam continuamente à sua réplica de produção.

Vejamos um caso simples em que você tem um aplicativo chamado Simple-Service que atualmente funciona 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 mais informações sobre como usar o AWS CLI, consulte a Referência de AWS CLI Comandos. Para conferir uma lista de ações da API de prontidão e links para mais informações, consulte Operações de API de verificação de prontidão.

As células no 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 ARC é um serviço global que oferece suporte a endpoints em vários 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 do ARC CLI. Por exemplo, para criar recursos como grupos de recuperação ou verificações de prontidão.

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 recurso de alto nível para prontidão para recuperação no 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 ARC, um grupo de recursos que você deseja monitorar é chamado de conjunto de recursos. 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 recursos.

Vamos supor que nosso Simple-Service O aplicativo é realmente muito simples e usa 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 recursos que reflita nosso Simple-Service recursos do aplicativo.

```
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 recursos de uma AWS conta. 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 recursos para modelar o Simple-Service aplicação em 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 ARC, use `list-rules` ou consulteDescrições das regras de prontidão no ARC. O ARC tem um conjunto específico de regras que ele executa para cada tipo de recurso; elas não são personalizáveis no momento.

4a. Crie uma verificação de prontidão para o conjunto de recursos, 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"
        }
    ]
}
```

Trabalhando com grupos de recuperação e verificações de prontidão

Esta seção descreve e fornece procedimentos para grupos de recuperação e verificações de prontidão, incluindo a criação, atualização e exclusão desses recursos.

Criando, atualizando e excluindo grupos de recuperação no ARC

Um grupo de recuperação representa seu aplicativo no Amazon Application Recovery Controller (ARC). 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 AWS região 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 ARC ajudam a determinar se seu 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 ARC para os recursos em seu aplicativo, para que o ARC possa ajudar a garantir que as réplicas tenham a mesma configuração ao longo do tempo.

Tópicos

- Criar grupos de recuperação
- Atualizar e excluir grupos e células de recuperação

Criar grupos de recuperação

As etapas desta seção explicam como criar um grupo de recuperação no console ARC. Para saber mais sobre o uso de operações de API de prontidão para recuperação com o Amazon Application Recovery Controller (ARC), consulte Operações de API de verificação de prontidão.

Como criar um grupo de recuperação

1. Abra o console ARC 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 Criar células e, em seguida, Adicionar célula.
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 ARC. Para saber mais sobre o uso de operações de API de prontidão para recuperação com o Amazon Application Recovery Controller (ARC), consulte Operações de API de verificação de prontidão.

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

1. Abra o console ARC 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.

Criando e atualizando verificações de prontidão no ARC

Esta seção fornece procedimentos para verificações de prontidão e conjuntos de recursos, incluindo a criação, atualização e exclusão desses recursos.

Criar e atualizar uma verificação de prontidão

As etapas desta seção explicam como criar uma verificação de prontidão no console ARC. Para saber mais sobre o uso de operações de API de prontidão para recuperação com o Amazon Application Recovery Controller (ARC), consulte Operações de API de 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 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 os 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 ARC espera para cada tipo de recurso, consulte. Tipos de recursos e formatos ARN em ARC

7. Se quiser, veja as regras de prontidão que serão usadas quando o ARC verificar o tipo de recurso que você incluiu nessa verificação de prontidão. 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 os escopos de prontidão aqui, o ARC não poderá retornar informações resumidas de prontidão para o grupo ou as células de recuperação.

9. Escolha Próximo.
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 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 ARC. Para saber mais sobre o uso de operações de API de prontidão para recuperação com o Amazon Application Recovery Controller (ARC), consulte Operações de API de verificação de prontidão.

Como criar um conjunto de recursos.

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/casa.
2. Em Controlador de recuperação de aplicações, escolha Conjuntos de recursos.
3. Escolha Criar.
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 do 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 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.

Monitorando o status de prontidão no ARC

Você pode ver a prontidão do seu aplicativo no Amazon Application Recovery Controller (ARC) 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 zona ou AWS região 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 usando os comandos ARC CLI.

Notificação de status de prontidão

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

Monitorando o status de prontidão no console ARC

O procedimento a seguir descreve como monitorar a prontidão de recuperação no AWS Management Console.

1. Abra o console ARC 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 AWS CLI comandos a serem usados 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
```

Obtendo recomendações de arquitetura no ARC

Se você já tem um aplicativo, o Amazon Application Recovery Controller (ARC) pode avaliar a arquitetura do seu aplicativo e as políticas de roteamento para fornecer recomendações para modificar o design para melhorar a resiliência de recuperação do seu aplicativo. Depois de criar um grupo de recuperação no 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 fornece informações adicionais, o ARC pode fornecer recomendações

melhores para você. Por exemplo, se você inserir um registro de recurso do Amazon Route 53 ou um Network Load Balancer como recurso de destino, o 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 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 ARC possa fornecer 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 em 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 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.

Criação de autorizações entre contas no ARC

Você pode ter seus recursos distribuídos em várias AWS contas, o que pode dificultar a obtenção de uma visão abrangente da integridade do seu aplicativo. Também pode dificultar a obtenção das informações necessárias para tomar decisões rápidas. Para ajudar a simplificar essa verificação de prontidão no Amazon Application Recovery Controller (ARC), você pode usar a autorização entre contas.

A autorização entre contas no ARC funciona com o recurso de verificação de prontidão. Com a autorização entre contas, você pode usar uma AWS conta central para monitorar seus recursos que estão localizados em várias AWS contas. 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 ARC para configurar e trabalhar com a autorização entre contas. Para ajudar você a começar, esta seção fornece exemplos de AWS CLI comandos.

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 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 tenha as seguintes AWS contas:

- 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 que tenha AWS recursos que você deseja adicionar e monitorar no ARC.

> **Note**
>
> O ARC é um serviço global que oferece suporte a endpoints em várias AWS regiões, mas você deve especificar a região Oeste dos EUA (Oregon) (ou seja, especificar o parâmetro `--region us-west-2`) na maioria dos comandos do ARC CLI.

O AWS CLI comando 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"
    ]
}
```

Regras de prontidão, tipos de recursos e ARNS

Esta seção inclui informações de referência sobre as regras de prontidão, as descrições e os tipos de recursos suportados, além do formato dos Amazon Resource Names (ARNs) que você usa para conjuntos de recursos.

Descrições das regras de prontidão no ARC

Esta seção lista as descrições das regras de prontidão para todos os tipos de recursos suportados pelo Amazon Application Recovery Controller (ARC). Para ver uma lista dos tipos de recursos suportados pelo ARC, consulteTipos de recursos e formatos ARN em ARC.

Você também pode visualizar as descrições das regras de prontidão no console do 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 ARC

Esta seção lista o conjunto de regras de prontidão para cada tipo de recurso suportado pelo 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 ARC define o status de prontidão, consulte Como as regras de prontidão determinam o status de prontidão.

Regras de prontidão

O 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 NOT READY.

- 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 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 ajuste de escala automático 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 balanceadores de carga clássicos para garantir que eles tenham pelo menos uma EC2 instância.
- 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 Classic Load Balancers para garantir que eles tenham o mesmo valor para o balanceador 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 da 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 tudo EBS volumes para garantir que tenham o mesmo valor para criptografia (HABILITADO ou DESATIVADO).
- EbsVolumeEncryptionDefault: Inspeciona tudo EBS volumes para garantir que eles tenham o mesmo valor para criptografia por padrão (HABILITADO ou DESATIVADO).
- EbsVolumeIops: Inspeciona tudo EBS volumes para garantir que eles tenham as mesmas operações de entrada/saída por segundo (IOPS).
- EbsVolumeKmsKeyId: Inspeciona tudo EBS volumes para garantir que eles tenham o mesmo ID de AWS KMS chave padrão.
- EbsVolumeMultiAttach: Inspeciona tudo EBS volumes para garantir que tenham o mesmo valor para conexão múltipla (HABILITADO ou DESATIVADO).
- EbsVolumeQuotas: Inspeciona tudo EBS volumes para garantir que estejam em conformidade com as cotas (limites) definidas pelas Cotas de Serviço.
- EbsVolumeSize: Inspeciona tudo EBS volumes para garantir que tenham o mesmo tamanho legível.
- EbsVolumeState: Inspeciona tudo EBS volumes para garantir que eles tenham o mesmo estado de volume.
- EbsVolumeType: Inspeciona tudo EBS volumes para garantir que eles tenham o mesmo tipo de volume.

AWS Lambda funções

- LambdaMemorySize: inspeciona todas as funções do Lambda para garantir que elas tenham o mesmo tamanho de memória. Se uma delas tiver mais memória, as outras serão marcadas como `NOT READY`.

- LambdaFunctionTimeout: inspeciona todas as funções do Lambda para garantir que elas tenham o mesmo valor de tempo limite. Se uma delas tiver um valor maior, as outras serão marcadas como `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 delas tiver um valor maior, as outras serão marcadas como `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 da 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 balanceadores de carga de rede e balanceadores de carga de aplicativos 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 MSK para garantir que eles tenham o mesmo tipo de EC2 instância da Amazon.
- 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 deles tiver um valor maior, os outros serão marcados como NOT READY.
- MskClusterACMCertificate: inspeciona todos os clusters MSK para garantir que eles tenham a mesma lista de certificados de autorização do cliente. ARNs
- 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 deles tiver um valor maior, os outros serão marcados como NOT READY.
- 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 AWS serviço, 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 do 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 tudo VPCs para garantir que todos tenham o mesmo valor para o tamanho da rede de blocos CIDR.
- VpcCidrBlocksSameProtocolVersion: inspeciona todos os VPCs que têm os mesmos blocos CIDR para garantir que tenham o mesmo valor para o número da versão do Internet Stream Protocol.
- VpcCidrBlocksStateInAssociationSets: inspeciona todos os conjuntos de associação de blocos CIDR VPCs para todos para garantir que todos tenham blocos CIDR em um estado. `ASSOCIATED`
- VpcIpv6CidrBlocksStateInAssociationSets: inspeciona todos os conjuntos de associação de blocos CIDR VPCs para todos para garantir que todos tenham blocos CIDR com o mesmo número de endereços.

- VpcCidrBlocksInAssociationSets: inspeciona todos os conjuntos de associação de blocos CIDR para todos VPCs para garantir que todos tenham o mesmo tamanho.
- VpcIpv6CidrBlocksInAssociationSets: inspeciona todos os conjuntos de associação de blocos IPv6 CIDR VPCs para garantir que tenham o mesmo tamanho.
- VpcState: inspeciona cada VPC para garantir que ela esteja em estado `AVAILABLE`.
- VpcInstanceTenancy: inspeciona tudo VPCs para garantir que todos tenham o mesmo valor para`Instance Tenancy`.
- VpcIsDefault: inspeciona tudo VPCs para garantir que 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.

AWS VPN conexões

- 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 VPN gateways

- 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 cada tipo de recurso.

Como visualizar as regras de prontidão no console

1. Abra o console ARC 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 em ARC

Ao criar um conjunto de recursos no Amazon Application Recovery Controller (ARC), você especifica o tipo de recurso a ser incluído no conjunto e os Amazon Resource Names (ARNs) para cada

um dos recursos a serem incluídos. O ARC espera um formato ARN específico para cada tipo de recurso. Esta seção lista os tipos de recursos suportados pelo ARC e os formatos ARN associados a cada um.

Os formatos específicos dependem do recurso. Ao fornecer um ARN, substitua o *italicized* texto pelas informações específicas do recurso.

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

AWS::ApiGateway::Stage

Um estágio do Amazon API Gateway versão 1.

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

  Example: `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`*

  Example: `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`

  Example: `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`

  Example: `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`

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

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

AWS::EC2::Volume

Um volume do Amazon EBS.

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

  Example: `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`

  Example: `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 AWS Lambda função.

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

  Example: `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`

  Example: `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`

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

  Para obter mais informações, consulte Trabalhando com nomes de recursos da Amazon (ARNs) no Amazon RDS.

AWS::Route53::HealthCheck

Uma verificação de integridade do Amazon Route 53.

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

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

AWS::SQS::Queue

Uma fila do Amazon SQS.

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

  Example: `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`

  Example: `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`

  Example: `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`

  Example: `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`

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

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

AWS::EC2::VPNGateway

Um gateway de rede privada virtual (VPN).

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

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

  Para obter mais informações, consulte Tipos de recursos definidos pela 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`

OBSERVAÇÃO: Você deve incluir o ID da conta na zona hospedada ARNs, conforme especificado aqui. O ID da conta é necessário para que o 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.

Registro e monitoramento para verificação de prontidão no Amazon Application Recovery Controller (ARC)

Você pode usar a Amazon CloudWatch e a Amazon EventBridge para monitorar a verificação de prontidão no Amazon Application Recovery Controller (ARC), para analisar padrões e ajudar a solucionar problemas. AWS CloudTrail

> **Note**
>
> Você deve visualizar CloudWatch métricas e registros do ARC na região Oeste dos EUA (Oregon), tanto no console quanto ao usar o. AWS CLI Ao usar o 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 verificação de prontidão no ARC
- Registrando chamadas de API de verificação de prontidão usando AWS CloudTrail
- Usando a verificação de prontidão no ARC com a Amazon EventBridge

Usando a Amazon CloudWatch com verificação de prontidão no ARC

O Amazon Application Recovery Controller (ARC) 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 AWS região durante um período de tempo especificado. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

É possível 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 ARC

O namespace `AWS/Route53RecoveryReadiness` inclui as métricas a seguir.

Métrica	Descrição
`ReadinessChecks`	Representa o número de verificações de prontidão processadas pelo ARC. A métrica pode ser dimensionada por seus estados, listados abaixo. Unidade: `Count`. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`.

Métrica	Descrição
	Dimensões • READY • NOT_READY • NOT_AUTHORIZED • UNKNOWN
Resources	Representa o número de recursos processados pelo ARC, que podem ser dimensionados pelo identificador do recurso, conforme definido pela API. Unidade: Count. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • ResourceSetType : Esses são os tipos de recursos, filtrados pelo número de recursos por determinado tipo avaliado pelo ARC Por exemplo: AWS::CloudWatch::Alarm

Estatísticas das métricas do ARC

CloudWatch fornece estatísticas com base nos pontos de dados métricos publicados pelo 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 ARC.
- Visualize o número total de recursos para um determinado tipo de conjunto de recursos avaliado pelo ARC.

Exibir CloudWatch métricas no ARC

Você pode visualizar as CloudWatch métricas do 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 ARC na região Oeste dos EUA (Oregon), tanto no console quanto ao usar o. AWS CLI Ao usar o 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 o 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 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"
        }
    ]
}
```

Registrando chamadas de API de verificação de prontidão usando AWS CloudTrail

é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no ARC. CloudTrail captura todas as chamadas de API para ARC como eventos. As chamadas capturadas incluem chamadas do console ARC e chamadas de código para as operações da API ARC.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para 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 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 sobre ARC em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no ARC, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do 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 eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do ARC são registradas CloudTrail e documentadas no Guia de referência da API Recovery Readiness para o Amazon Application Recovery Controller, no Guia de referência da API de configuração de controle de recuperação para o Amazon Application Recovery Controller e no Guia de referência da API Routing Control para o Amazon 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 o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Visualizando eventos ARC no histórico de eventos

CloudTrail permite que você visualize eventos recentes no histórico de eventos. Para visualizar eventos para solicitações da API 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.

Entendendo as entradas do arquivo de log 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 `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"
}
```

Usando a verificação de prontidão no ARC com a Amazon EventBridge

Usando a Amazon EventBridge, você pode configurar regras orientadas por eventos que monitoram seus recursos de verificação de prontidão no Amazon Application Recovery Controller (ARC) e, em seguida, iniciar 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 o status de uma verificação de prontidão muda de PRONTO para NÃO PRONTO.

> **Note**
>
> O ARC publica somente EventBridge eventos para verificação de prontidão na região Oeste dos EUA (Oregon) (us-west-2). AWS Para receber EventBridge eventos para verificação de prontidão, crie EventBridge regras na região Oeste dos EUA (Oregon).

Você pode criar regras na Amazon EventBridge para atuar no seguinte evento de verificação de prontidão do ARC:

- Prontidão verifica prontidão. O evento especifica se o status da verificação de prontidão muda, por exemplo, de PRONTO para NOT READY.

Para capturar eventos ARC específicos 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 ARC para 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 de verificação de prontidão com EventBridge

Com EventBridge, você pode criar regras que definem as ações a serem tomadas quando o ARC emite eventos para recursos de verificação de prontidão.

Para digitar ou copiar e colar um padrão de evento no EventBridge console, no console, selecione a opção Inserir minha própria opção. Para ajudá-lo a determinar padrões de eventos que podem ser úteis para você, este tópico inclui exemplos de padrões de eventos de prontidão.

Para criar uma regra para um evento de recurso

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. Para criar Região da AWS a regra em, escolha Oeste dos EUA (Oregon). Essa é a região necessária para eventos de preparação.
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. Para ver exemplos, consulte a próxima seção.

Exemplos de padrões de eventos de prontidão

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.

Os padrões de eventos a seguir fornecem exemplos que você pode usar EventBridge para o recurso de verificação de prontidão no ARC.

- Selecione todos os eventos da verificação de prontidão do 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"
            }
         ]
      }
   }
}
```

Veja a seguir um exemplo de evento 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 exemplo de evento ARC para uma alteração no status de prontidão da 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 exemplo de evento ARC para uma mudança 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 de prontidão, consulte Monitorar um recurso de verificação de prontidão com. EventBridge
4. Na página Selecionar destino, escolha CloudWatchcomo seu alvo.
5. Escolha um grupo de CloudWatch registros no menu suspenso.

Identity and Access Management para verificação de prontidão

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 (conectado) e autorizado (tem permissões) para usar os recursos do ARC. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Conteúdo

Como o readiness check in SERVICElong; funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao ARC, saiba quais recursos do IAM estão disponíveis para uso com o ARC.

Antes de usar o IAM para gerenciar o acesso à verificação de prontidão no Amazon Application Recovery Controller (ARC), saiba quais recursos do IAM estão disponíveis para uso com a verificação de prontidão.

Recursos do IAM que você pode usar com verificação de prontidão no Amazon Application Recovery Controller (ARC)

Atributo do IAM	Suporte para verificação de prontidão
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim

Atributo do IAM	Suporte para verificação de prontidão
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para obter uma visão geral de alto nível de como os AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS Serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para verificação de prontidão

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 do IAM, grupo de usuários ou perfil. 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 Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim 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 perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Para ver exemplos de políticas baseadas em identidade do ARC, consulte. Exemplos de políticas baseadas em identidade no Amazon Application Recovery Controller (ARC)

Políticas baseadas em recursos dentro da verificação de prontidão

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos 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 políticas para verificação de prontidão

Compatível com 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 podem ser usadas 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. Algumas operações também 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 de ações do ARC para verificação de prontidão, consulte Ações definidas pelo Amazon Route 53 Recovery Readiness na Referência de Autorização de Serviço.

As ações de política no ARC para verificação de prontidão usam os seguintes prefixos antes da ação:

```
route53-recovery-readiness
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas. Por exemplo, o seguinte:

```
"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 ver exemplos de políticas baseadas em identidade do ARC para verificação de prontidão, consulte. Exemplos de políticas baseadas em identidade para verificação de prontidão no Amazon Application Recovery Controller (ARC)

Recursos de políticas para verificação de prontidão

Compatível com 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 de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista de ações do ARC para mudança de zona, consulte Ações definidas pelo Amazon Route 53 Recovery Readiness.

Para ver exemplos de políticas baseadas em identidade do ARC para verificação de prontidão, consulte. Exemplos de políticas baseadas em identidade para verificação de prontidão no Amazon Application Recovery Controller (ARC)

Chaves de condição de política para verificação de prontidão

Compatível com chaves de condição de política específicas de 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 `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `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 antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar 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 da 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 ações do ARC para verificação de prontidão, consulte Chaves de condição para preparação de recuperação do Amazon Route 53

Para ver as ações e os recursos que você pode usar com uma chave de condição com verificação de prontidão, consulte Ações definidas pelo Amazon Route 53 Recovery Readiness

Para ver exemplos de políticas baseadas em identidade do ARC para verificação de prontidão, consulte. Exemplos de políticas baseadas em identidade para verificação de prontidão no Amazon Application Recovery Controller (ARC)

Listas de controle de acesso (ACLs) na verificação de prontidão

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso baseado em atributos (ABAC) com verificação de prontidão

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as 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. Marcar de entidades e atributos 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 estiver 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 chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do 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.

A prontidão de recuperação (verificação de prontidão) suporta ABAC.

Usando credenciais temporárias com verificação de prontidão

Compatível com 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 “Trabalhe 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 funções, consulte Alternar para um perfil do IAM (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 principais entre serviços para verificação de prontidão

Compatibilidade com o recurso de 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. Permissões concedidas por políticas a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, acionar outra ação em outro serviço. Nesse caso, você precisa ter permissões para executar ambas as ações.

Para ver se uma ação na verificação de prontidão exige ações dependentes adicionais em uma política, consulte Prontidão de recuperação do Amazon Route 53

Funções de serviço para verificação de prontidão

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar 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.

Funções vinculadas ao serviço para verificação de prontidão

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço ARC, consulte. Usando a função vinculada ao serviço para verificação de prontidão no ARC

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para verificação de prontidão no Amazon Application Recovery Controller (ARC)

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos ARC. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos

recursos 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 aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo ARC, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon Application Recovery Controller (ARC) na Referência de autorização de serviço. ARNs

Tópicos

- Práticas recomendadas de política
- Exemplo: verificação de prontidão no acesso ao console
- Exemplos: ações da API de verificação de prontidão para verificação de prontidão

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos ARC em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance 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 funções 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 da 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 cem verificações de política e recomendações práticas para ajudar 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 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: verificação de prontidão no acesso ao console

Para acessar o console do Amazon Application Recovery Controller (ARC), você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do ARC em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva 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 à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console de verificação de prontidão quando você permite acesso somente a operações específicas de API, anexe também uma política `ReadOnly` AWS gerenciada para verificação de prontidão às entidades. Para obter mais informações, consulte a página de políticas gerenciadas da verificação de prontidão Verificação de prontidão ou Adicionar permissões a um usuário no Guia do usuário do IAM.

Para realizar algumas tarefas, os usuários devem ter permissão para criar a função vinculada ao serviço associada à verificação de prontidão no ARC. Para saber mais, consulte Usando a função vinculada ao serviço para verificação de prontidão no ARC.

Para dar aos usuários acesso total ao uso dos recursos de verificação de prontidão por meio do console, 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:UpdateCell",
                   "route53-recovery-readiness:UpdateReadinessCheck",
                   "route53-recovery-readiness:UpdateRecoveryGroup",
                   "route53-recovery-readiness:UpdateResourceSet"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Exemplos: ações da API de verificação de prontidão para verificação de prontidão

Para garantir que um usuário possa usar as ações da API ARC para trabalhar com o plano de controle de verificação de prontidão do ARC — por exemplo, para criar grupos de recuperação, conjuntos de recursos e verificações de prontidão — anexe uma política que corresponda às operações da API com as quais o usuário precisa trabalhar, conforme descrito abaixo.

Para realizar algumas tarefas, os usuários devem ter permissão para criar a função vinculada ao serviço associada à verificação de prontidão no ARC. Para saber mais, consulte Usando a função vinculada ao serviço para verificação de prontidão no ARC.

Para trabalhar com operações de API para verificação de prontidão, 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": "*"
        }
    ]
}
```

Usando a função vinculada ao serviço para verificação de prontidão no ARC

O Amazon Application Recovery Controller usa funções vinculadas a serviços AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a um serviço — nesse caso, ARC. As funções vinculadas ao serviço são predefinidas pelo ARC e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome para fins específicos.

As funções vinculadas ao serviço facilitam a configuração do ARC porque você não precisa adicionar manualmente as permissões necessárias. O ARC define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o ARC pode assumir suas funções. 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 ARC porque você não pode remover inadvertidamente a permissão 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 para esse serviço.

O ARC tem as seguintes funções vinculadas ao serviço, descritas neste capítulo:

- O ARC usa a função vinculada ao serviço chamada Route53 RecoveryReadinessServiceRolePolicy para acessar recursos e configurações para verificar a prontidão.
- O ARC usa a função vinculada ao serviço nomeada para 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 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.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Criando a função vinculada ao RecoveryReadinessServiceRolePolicy serviço Route53 para 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 ARC cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria a primeira verificação de prontidão ou autorização entre contas, o ARC cria a função vinculada ao serviço para você novamente.

Editando a função vinculada ao RecoveryReadinessServiceRolePolicy serviço Route53 para ARC

O 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 obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo a função vinculada ao RecoveryReadinessServiceRolePolicy serviço Route53 para ARC

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de seu perfil vinculado ao serviço antes de excluí-lo 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 no ARC. Para obter informações sobre autorizações entre contas, consulte Criação de autorizações entre contas no ARC.

> **Note**
>
> Se o serviço ARC estiver usando a função quando você tentar excluir os recursos, a exclusão da função 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.

Atualizações na função vinculada ao serviço ARC para verificação de prontidão

Para atualizações das políticas AWS gerenciadas para as funções vinculadas ao serviço ARC, consulte a tabela de atualizações de políticas AWS gerenciadas para ARC. Você também pode assinar alertas automáticos de RSS na página de histórico do documento ARC.

AWS políticas gerenciadas para verificação de prontidão no Amazon Application Recovery Controller (ARC)

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 elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são 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 Políticas gerenciadas pela AWS no Guia do usuário do IAM.

AWS política gerenciada: Route53 RecoveryReadinessServiceRolePolicy

Não é possível anexar a `Route53RecoveryReadinessServiceRolePolicy` às entidades do IAM. Essa política está vinculada a uma função vinculada a serviços que permite que o Amazon Application Recovery Controller (ARC) acesse AWS serviços e recursos que são usados ou gerenciados pelo ARC. Para obter mais informações, consulte Usando a função vinculada ao serviço para verificação de prontidão no ARC.

AWS política gerenciada: AmazonRoute 53 RecoveryReadinessFullAccess

Você pode anexar `AmazonRoute53RecoveryReadinessFullAccess` às entidades do IAM. Esta política concede acesso total às ações para trabalhar com prontidão para recuperação (verificação de prontidão) no 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. Essa política concede acesso somente de leitura às ações para trabalhar com prontidão para recuperação no 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.

Atualizações de políticas AWS gerenciadas para prontidão

Para obter detalhes sobre atualizações nas políticas AWS gerenciadas para verificação de prontidão no ARC desde que esse serviço começou a rastrear essas alterações, consulteAtualizações nas políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC). Para alertas automáticos sobre alterações nesta página, assine o feed RSS na página de histórico do documento ARC.

Cotas para verificação de prontidão

A verificação de prontidão no Amazon Application Recovery Controller (ARC) está sujeita às seguintes cotas (anteriormente chamadas de limites).

Entidade	Quota
Número de grupos de recuperação por conta	5
Número de células por conta	15

Entidade	Quota
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

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 perfis de serviço individuais, você pode ver as ações no contexto em seus cenários relacionados.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando esse serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Exemplos de código

- Exemplos básicos do Application Recovery Controller usando AWS SDKs
  - Ações para o Application Recovery Controller usando AWS SDKs
    - Use GetRoutingControlState com um AWS SDK
    - Use UpdateRoutingControlState com um AWS SDK

Exemplos básicos do Application Recovery Controller usando AWS SDKs

Os exemplos de código a seguir mostram como usar os conceitos básicos do Amazon Route 53 Application Recovery Controller com AWS SDKs.

Exemplos

- Ações para o Application Recovery Controller usando AWS SDKs
  - Use GetRoutingControlState com um AWS SDK
  - Use UpdateRoutingControlState com um AWS SDK

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. 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

- Use GetRoutingControlState com um AWS SDK
- Use UpdateRoutingControlState com um AWS SDK

Use **`GetRoutingControlState`** com um AWS SDK

Os exemplos de código a seguir mostram como usar o `GetRoutingControlState`.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
    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 Repositório de exemplos de código da AWS.

```
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, consulteUsando esse serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **UpdateRoutingControlState** com um AWS SDK

Os exemplos de código a seguir mostram como usar o `UpdateRoutingControlState`.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
    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 Repositório de exemplos de código da AWS.

```
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, consulteUsando esse serviço com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Segurança no Amazon Application Recovery Controller

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 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 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 você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o ARC. Os tópicos a seguir mostram como configurar o ARC 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.

Tópicos

Proteção de dados no Amazon Application Recovery Controller

O modelo de responsabilidade AWS compartilhada O modelo se aplica à proteção de dados no Amazon 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 o 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 Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD 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 AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- 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 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o ARC ou outro Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em 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, recomendamos 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 ARC são gravados em um volume do Amazon EBS para backup. O 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 ARC, consultas de status de prontidão, atualizações do estado da célula etc. — são criptografadas durante o transporte em todo o serviço usando o TLS.

Identity and Access Management para Amazon Application Recovery Controller (ARC)

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 (conectado) e autorizado (tem permissões) para usar os recursos do ARC. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no ARC.

Usuário do serviço — Se você usar o serviço ARC para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do ARC para fazer seu trabalho, talvez precise de permissões adicionais. Compreenda como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se

você não conseguir acessar um recurso no ARC, consulteSolução de problemas de identidade e acesso do .

Administrador de serviços — Se você é responsável pelos recursos do ARC em sua empresa, provavelmente tem acesso total ao ARC. É seu trabalho determinar quais recursos e recursos do ARC seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com o ARC, consulteComo os recursos do Amazon Application Recovery Controller (ARC) funcionam com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao ARC. Para ver exemplos de políticas baseadas em identidade ARC que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade no Amazon Application Recovery Controller (ARC)

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login 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 designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer 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 da AWS no IAM 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 puder 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, é recomendável 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 .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com 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, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar 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 IAMAdminse conceder 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 Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil 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, é possível 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 por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM 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 presumir 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 conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na 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 um perfil vinculado 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 Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar 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 presumir o perfil para 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 editar as permissões para perfis vinculados a serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias.

Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

Gerenciar o 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 perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos 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.

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 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 Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas 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 recursos

Políticas baseadas em recursos 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 atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo 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 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 diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a 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 recurso 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 com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil 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 recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas 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 Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- 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 recursos. 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 os recursos do Amazon Application Recovery Controller (ARC) funcionam com o IAM

Para obter informações sobre como cada recurso do Amazon Application Recovery Controller (ARC) funciona com o IAM, consulte os seguintes tópicos:

- IAM para mudança zonal
- IAM para mudança automática zonal
- IAM para controle de roteamento
- IAM para verificação de prontidão

Exemplos de políticas baseadas em identidade no Amazon Application Recovery Controller (ARC)

Para ver exemplos de políticas baseadas em identidade para cada recurso no Amazon Application Recovery Controller (ARC), consulte os seguintes tópicos nos AWS Identity and Access Management capítulos de cada recurso:

- Exemplos de políticas baseadas em identidade para mudança automática zonal
- Exemplos de políticas baseadas em identidade para mudança zonal no ARC
- Exemplos de políticas baseadas em identidade para controle de roteamento no Amazon Application Recovery Controller (ARC)
- Exemplos de políticas baseadas em identidade para verificação de prontidão no Amazon Application Recovery Controller (ARC)

AWS políticas gerenciadas para o Amazon Application Recovery Controller (ARC)

Para obter informações sobre as políticas AWS gerenciadas para os recursos do ARC com políticas gerenciadas, incluindo uma política gerenciada para uma função vinculada ao serviço, consulte os seguintes tópicos:

- Políticas gerenciadas para mudança automática zonal
- Políticas gerenciadas para controle de roteamento
- Políticas gerenciadas para verificação de prontidão

Atualizações nas políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC)

Veja detalhes sobre as atualizações das políticas AWS gerenciadas para recursos no ARC desde que esse serviço começou a rastrear essas alterações. Para alertas automáticos sobre alterações nesta página, assine o feed RSS na página de histórico do documento ARC.

Alteração	Descrição	Data
AWSZonalAutoshiftPracticeRunSLRPolicy política gerenciada — Política atualizada	Adiciona a declaração de política `Autoshift PracticeCheckPermissions` com as permissões `sautoscaling:DescribeAutoScalingGroups`, `ec2:DescribeInstances` `elasticloadbalancing:DescribeTargetHealth`, e `elasticloadbalancing:DescribeTargetHealth` para apoiar verificações de capacidade balanceada. Para saber mais, consulte Como a mudança automática de zona e as execuções práticas funcionam.	30 de junho de 2025
AWSServiceRoleForPercPracticePolicy— Nova política	O ARC adicionou uma nova função vinculada a serviços para mudanças automáticas e execuções práticas. O ARC usa as permissões habilitadas pela função vinculada ao serviço para	30 de novembro de 2023

Alteração	Descrição	Data
	monitorar os alarmes e eventos do cliente CloudWatch da Amazon fornecidos pelo AWS Health Dashboard cliente para os treinos e para iniciar os treinos. Para saber mais sobre o novo perfil vinculado ao serviço, consulte Permissões de função vinculadas ao serviço para AWSService RoleForZonalAutoshiftPracticeRun.	
AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Política atualizada	Adiciona permissões para`GetResourcePolicy` , para apoiar o retorno de detalhes sobre políticas AWS Resource Access Manager de recursos para recursos compartilhados.	18 de outubro de 2023

Alteração	Descrição	Data

Route53 RecoveryReadinessServiceRolePolicy — Política atualizada	O ARC adicionou novas permissões para consultar informações sobre EC2 instâncias da Amazon.
	
	O ARC usa as seguintes permissões para apoiar a pesquisa de EC2 instâncias da Amazon, executar verificações de prontidão e determinar o status de prontidão das instâncias.
	
	`ec2:DescribeVpnGateways`
	
	`ec2:DescribeCustomerGateways`
		17 de fevereiro de 2023

Route53 RecoveryReadinessServiceRolePolicy — Política atualizada	O ARC adicionou uma nova permissão para consultar informações sobre as funções do Lambda. O 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. `lambda:ListProvisionedConcurrencyConfigs`	31 de agosto de 2022

Alteração	Descrição	Data
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
AmazonRoute53 RecoveryClusterReadOnlyAccess — Política atualizada	O ARC adicionou uma nova permissão, `route53-recovery-cluster:ListRoutingControls` , para permitir o controle de roteamento de listagem ARNs com alta disponibilidade.	15 de março de 2022
AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Política atualizada	O ARC adicionou uma nova permissão, `route53-recovery-control-config:ListTagsForResources` , para permitir a listagem de tags para um recurso.	20 de dezembro de 2021

Alteração	Descrição	Data
Route53 RecoveryReadinessServiceRolePolicy — Política atualizada	O ARC adicionou uma nova permissão para consultar informações sobre o Amazon API Gateway. O 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
AmazonRoute53 RecoveryReadinessReadOnlyAccess — Novas permissões adicionadas	O ARC adicionou duas novas permissões a AmazonRoute53 RecoveryReadinessReadOnlyAccess: O ARC usa `route53-recovery-readiness:GetArchitectureRecommendations` e `route53-recovery-readiness:GetCellReadinessSummary` permite acesso somente de leitura a essas ações para trabalhar com prontidão para recuperação.	15 de outubro de 2021

Alteração	Descrição	Data

Route53 RecoveryReadinessServiceRolePolicy — Política atualizada	O ARC adicionou novas permissões para consultar informações sobre as funções do Lambda.
	
	O 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.
	
	`lambda:GetFunctionConcurrency`
	
	`lambda:GetFunctionConfiguration`
	
	`lambda:GetProvisionedConcurrencyConfig`
	
	`lambda:ListAliases`
	
	`lambda:ListVersionsByFunction`
	
	`lambda:ListEventSourceMappings`
	
	`lambda:ListFunctions`
		8 de outubro de 2021

Alteração	Descrição	Data
Route53 RecoveryReadinessServiceRolePolicy — Novas políticas gerenciadas adicionadas	O ARC adicionou as seguintes novas políticas gerenciadas: AmazonRoute53 RecoveryReadinessFullAccess AmazonRoute53 RecoveryReadinessReadOnlyAccess AmazonRoute53 RecoveryClusterFullAccess AmazonRoute53 RecoveryClusterReadOnlyAccess AmazonRoute53 RecoveryControlConfigFullAccess AmazonRoute53 RecoveryControlConfigReadOnlyAccess	18 de agosto de 2021
O ARC começou a rastrear as mudanças	A ARC começou a monitorar as mudanças em suas políticas AWS gerenciadas.	27 de julho de 2021

Solução de problemas de identidade e acesso do

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Amazon Application Recovery Controller (ARC) e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no ARC
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do ARC

Não estou autorizado a realizar uma ação no 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 um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o 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 exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no ARC. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil 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 do ARC

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível 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 ARC suporta esses recursos, consulteComo os recursos do Amazon Application Recovery Controller (ARC) funcionam 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 perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Registro e monitoramento no ARC

O monitoramento é uma parte importante da manutenção da disponibilidade e do desempenho do ARC 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 multiponto, caso ocorra. AWS fornece várias ferramentas para monitorar seus recursos e atividades do ARC e responder a possíveis incidentes, por exemplo, e a AWS CloudTrail Amazon. CloudWatch

Para obter informações sobre o monitoramento de cada recurso no ARC, consulte os seguintes tópicos:

- Registro e monitoramento para mudança zonal
- Registro e monitoramento para mudança automática zonal
- Registro e monitoramento para controle de roteamento

- Registro e monitoramento para verificação de prontidão

Validação de conformidade para o Amazon Application Recovery Controller

Auditores terceirizados avaliam a segurança e a conformidade do Amazon 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:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a 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.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- 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 no Amazon Application Recovery Controller

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 altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center 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 ARC oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Segurança da infraestrutura no Amazon Application Recovery Controller

Como serviço gerenciado, 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 ARC pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Histórico de documentos do Guia do desenvolvedor do Amazon Application Recovery Controller (ARC)

As entradas a seguir descrevem mudanças importantes feitas na documentação do Amazon Application Recovery Controller (ARC).

- Versão: mais recente
- Última atualização da documentação: 30 de junho de 2025

Alteração	Descrição	Data
Aprimoramentos na prática de corridas	Agora você pode iniciar execuções práticas sob demanda no ARC. Além disso, os treinos agora incluem verificações de capacidad e suficiente AZs em outras áreas da região. Para obter mais informações, consulte Como funciona.	30 de junho de 2025
Política gerenciada atualizada	Atualiza a política `AWSZonalA utoshiftPracticeRu nSLRPolicy` gerenciad a adicionando a declaraçã o de política `Autoshift PracticeCheckPermi ssions` com as permissõe `sautoscaling:Descri beAutoScalingGroup s` ,, `ec2:DescribeInstan ces elasticlo adbalancing:Descri beTargetHealth` , e	30 de junho de 2025

Alteração	Descrição	Data
	`elasticloadbalancing:DescribeTargetHealth` para dar suporte às verificações de capacidade balanceada. Para obter mais informações, consulte política AWSZonalAutoshiftPracticeRunSLRPolicy gerenciada.	
Atualizações nos tipos de exceção para o deslocamento automático zonal	Agora você pode interagir com o deslocamento automático zonal por recurso. Para obter mais informações, consulte Como funciona.	21 de abril de 2025
Teste o deslocamento automático zonal ARC com AWS FIS	Você pode usar AWS FIS para testar como o deslocamento automático zonal ARC recupera automaticamente seu aplicativo durante uma interrupção de alimentação do AZ Para obter mais informações, consulte Testando o deslocamento automático zonal com. AWS FIS	26 de março de 2025

Alteração	Descrição	Data
O ARC agora oferece suporte a IPv6 endpoints para controles de roteamento e mudança zonal.	O ARC agora oferece suporte a IPv6 endpoints para controles de roteamento e mudança zonal. Para obter mais informaçõ es, consulte Configurar componentes de controle de roteamento.	21 de novembro de 2024
Capacidade de mudança zonal para grupos do Amazon EC2 Auto Scaling	O ARC agora oferece suporte à mudança de zona para grupos do Amazon EC2 Auto Scaling. Para obter mais informações, consulte Support for Amazon EC2 Auto Scaling groups.	18 de novembro de 2024

Alteração	Descrição	Data
Capacidade de mudança zonal para o Amazon EKS	Você pode iniciar uma mudança zonal para um cluster Amazon EKS ou permitir que ela seja feita por você ativando AWS a mudança automática zonal. Essa mudança atualiza o fluxo de tráfego de east-to-west rede em seu cluster para considerar apenas os endpoints de rede para pods executados em nós de trabalho em bom estado. AZs Para obter mais informações, consulte Support for Amazon Elastic Kubernetes Service (Amazon Elastic Kubernetes Service).	22 de outubro de 2024
Capacidade de mudança de zona para balanceadores de carga de rede	O ARC agora oferece suporte à mudança de zona para balanceadores de carga de rede com configurações entre zonas habilitadas ou desabilitadas entre zonas. Para obter mais informações, consulte Support for Network Load Balancers.	11 de outubro de 2024

Alteração	Descrição	Data
Notificações do observador do Autoshift	Com as notificações do observador de deslocamento automático, você pode configurar o deslocamento automático zonal para notificá-lo, por meio da Amazon EventBridge, sempre que AWS iniciar um deslocamento automático para afastar o tráfego de uma zona de disponibilidade potencialmente prejudicada. Você não precisa configurar nenhum recurso específico com o deslocamento automático zonal para ativar essas notificações separadas. Para obter mais informações, consulte Usando o deslocamento automático zonal com a Amazon. EventBridge	12 de julho de 2024

Alteração	Descrição	Data
Reorganização de documentos por cada recurso	Reorganiza o conteúdo do guia do desenvolvedor para ser dividido em guias de subdesenvolvedores. Ou seja, agora há seções separadas que contêm informações abrangentes para cada recurso no ARC: mudança zonal e mudança automática zonal para recuperação Multi-AZ e controle de roteamento e verificação de prontidão para recuperação multirregional. Para obter mais informações, consulte O que é o Amazon Application Recovery Controller (ARC).	30 de abril de 2024
Adiciona o recurso de mudança automática de zona	Adiciona um novo recurso no ARC em que você AWS autoriza a transferência do tráfego de recursos para um aplicativo de uma zona de disponibilidade, em seu nome, para ajudar a reduzir o tempo de recuperação durante eventos. Para obter mais informações, consulte Mudança automática zonal no Amazon Application Recovery Controller (ARC).	30 de novembro de 2023

Alteração	Descrição	Data
Adiciona um novo perfil vinculado ao serviço	Adiciona uma nova função vinculada ao serviço, AWSServiceRoleForZonalAutoshiftPracticeRun, para execuções práticas de mudança automática zonal. Para obter mais informações, consulte Service-linked role permissions for AWSServiceRoleForZonalAutoshiftPracticeRun.	30 de novembro de 2023
Adiciona compatibilidade entre contas com clusters	Adiciona suporte entre contas para clusters no ARC com AWS Resource Access Manager, para que você possa usar um cluster com facilidade e segurança para hospedar painéis de controle e controles de roteamento pertencentes a várias contas diferentes. AWS Para obter mais informações, consulte Support cross-account for clusters no ARC.	18 de outubro de 2023

Alteração	Descrição	Data
Política gerenciada atualizada	Atualiza a política `AmazonRoute53RecoveryControlConfigReadOnly` gerenciada para adicionar permissões e oferecer suporte ao retorno de detalhes sobre políticas AWS Resource Access Manager de recursos para recursos compartilhados. `GetResourcePolicy` Para obter mais informações, consulte Políticas gerenciadas pela AWS.	19 de setembro de 2023
Atualização do perfil vinculado ao serviço	Foram adicionadas novas permissões `ec2:DescribeVpnGateways` `eec2:DescribeCustomerGateways` , à função vinculada ao serviço do ARC, para apoiar a pesquisa de instâncias da Amazon EC2 . Para obter mais informações, consulte Usando funções vinculadas a serviços para ARC.	17 de fevereiro de 2023

Alteração	Descrição	Data
Versão GA para mudança de zona	Suporta a versão GA da mudança zonal para ARC, que inclui controle de acesso baseado em atributos (ABAC) para recursos gerenciados que são registrados no ARC para mudança zonal. Para obter mais informações, consulte Controle de acesso baseado em atributos (ABAC) com ARC.	10 de janeiro de 2023
Foi adicionada uma nova mudança de zona Multi-AZ	Conteúdo adicionado descrevendo um novo serviço em ARC, mudança zonal, para aplicativos Multi-AZ. É possível iniciar uma mudança de zona para mover temporari amente o tráfego de um recurso do balanceador de carga para fora de uma zona de disponibilidade. Para obter mais informações, consulte Mudança zonal no ARC.	28 de novembro de 2022

Alteração	Descrição	Data
Atualização do perfil vinculado ao serviço	Foi adicionada uma nova permissão,`lambda:ListProvisionedConcurrencyConfigs` , à função vinculada ao serviço do ARC para consultar informações sobre as funções do Lambda. Para obter mais informações, consulte Usando funções vinculadas a serviços para ARC.	31 de agosto de 2022
Política gerenciada pela atualizada	Atualizou a política gerenciada `AmazonRoute53RecoveryControlConfigFullAccess` para remover as permissões do Amazon Route 53 e listá-las como opcionais. Para obter mais informações, consulte as políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC).	26 de maio de 2022

Alteração	Descrição	Data
Política gerenciada pela atualizada	Atualizou a política gerenciada `AmazonRoute53RecoveryControlConfigFullAccess` para incluir as permissões necessárias do Amazon Route 53. Para obter mais informações, consulte as políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC).	15 de abril de 2022
Adicionado um exemplo de CLI para a nova API de listagem de controles de roteamento	Foram adicionados exemplos de comandos CLI e recomendações de melhores práticas para a nova operação da API de controles de roteamento de listas incluída na API de plano de dados ARC extremamente confiável. Para obter mais informações, consulte Listar e atualizar controles e estados de roteamento.	31 de março de 2022

Alteração	Descrição	Data
Adicionado o suporte para sobrepor regras de segurança	Foi adicionada compatibilidade 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. Para obter mais informações, consulte Sobrepor regras de segurança para redirecionar o tráfego.	2 de março de 2022
Agregado suporte adicional de marcação	Foi adicionado suporte para marcar recursos adicionais no ARC, incluindo clusters, painéis de controle, controles de roteamento e regras de segurança. Para obter mais informações, consulte Marcação no Amazon Application Recovery Controller (ARC).	20 de dezembro de 2021

Alteração	Descrição	Data
Política gerenciada pela atualizada	A política gerenciada `AmazonRoute53RecoveryControlConfigReadOnly` foi atualizada para adicionar permissão para listar as tags de um recurso. Para obter mais informações, consulte as políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC)	20 de dezembro de 2021
Suporte adicional para alertas em tempo real com EventBridge	Foi adicionado suporte para EventBridge, o que significa que agora você pode adicionar regras para receber alertas e agir de acordo com as alterações de status da verificação de prontidão do ARC, por exemplo, quando um status muda de PRONTO para NÃO PRONTO. Para obter mais informações, consulte Usando o ARC com a Amazon EventBridge.	20 de dezembro de 2021

Alteração	Descrição	Data
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. Para obter mais informações, consulte exemplos de API para o Amazon Application Recovery Controller (ARC).	16 de novembro de 2021
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` . Para obter mais informações, consulte as políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC).	9 de novembro de 2021

Alteração	Descrição	Data
Adicionada compatibilidade 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 ARC para que o ARC possa auditar o API Gateway com verificaç ões de prontidão. Para obter mais informações, consulte Regras de prontidão e tipos de recursos suportados e Uso de funções vinculadas a serviços para ARC.	28 de outubro de 2021
Foi adicionada compatibi lidade para o tipo de recurso de funções do Lambda	Adicionou um novo tipo de recurso, funções Lambda, e atualizou as permissões de função vinculadas ao serviço ARC para que o ARC possa auditar funções do Lambda com verificações de prontidão. Para obter mais informações, consulte Regras de prontidão e tipos de recursos suportados e Uso de funções vinculadas a serviços para ARC.	8 de outubro de 2021

Alteração	Descrição	Data
Links adicionados CloudFormation e modelos do Terraform	Links adicionados para baixar AWS CloudFormation e modelos do Hashicorp Terraform para ajudar você a começar a usar o Arc rapidamente. Para obter mais informações, consulte Preparação para recuperação com um novo aplicativo.	13 de setembro de 2021
Novas políticas gerenciadas adicionadas	Foram adicionadas as seguintes políticas AWS gerenciadas para ARC: `AmazonRoute53RecoveryReadinessFullAccess` `AmazonRoute53RecoveryReadinessReadOnlyAccess` `AmazonRoute53RecoveryClusterFullAccess` ,`AmazonRoute53RecoveryClusterReadOnlyAccess` ,`AmazonRoute53RecoveryControlConfigFullAccess` ,, `AmazonRoute53RecoveryControlConfigReadOnlyAccess` e. Para obter mais informações, consulte as políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC).	18 de agosto de 2021

Alteração	Descrição	Data
Começou a rastrear políticas AWS gerenciadas para o Amazon Application Recovery Controller (ARC)	As atualizações das políticas gerenciadas serão monitoradas a partir da data de lançamento inicial. Para obter mais informações, consulte as políticas AWS gerenciadas do Amazon Application Recovery Controller (ARC).	27 de julho de 2021
Lançamento inicial do Amazon Application Recovery Controller (ARC)	O ARC melhora a disponibilidade dos aplicativos ao coordenar centralmente os failovers em uma AWS região ou em várias regiões. O ARC fornece verificações de prontidão para garantir que seus aplicativos sejam dimensionados 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 obter mais informações, consulte O que é ARC? .	27 de julho de 2021

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.