Manual do usuário

AWS Hub de resiliência

AWS Hub de resiliência: Manual do usuário

Table of Contents

O que é AWS Resilience Hub?

AWS Resilience Hub é um local central para você gerenciar e melhorar a postura de resiliência de seus aplicativos. AWS AWS Resilience Hub permite que você defina suas metas de resiliência, avalie sua postura de resiliência em relação a essas metas e implemente recomendações de melhoria com base no AWS Well-Architected Framework. AWS Resilience Hub Nele, você também pode criar e executar experimentos do Amazon Fault Injection Service, que imitam interrupções reais em seu aplicativo para ajudá-lo a entender melhor as dependências e descobrir possíveis pontos fracos. AWS Resilience Hub fornece um local central com todos os AWS serviços e ferramentas de que você precisa para fortalecer continuamente sua postura de resiliência. AWS Resilience Hub trabalha com outros serviços para fornecer recomendações e ajudar você a gerenciar os recursos do seu aplicativo. Para obter mais informações, consulte Como trabalhar com outros serviços do .

A tabela a seguir fornece os links da documentação de todos os serviços de resiliência relacionados.

Serviços AWS e referências de resiliência relacionados

AWS serviço de resiliência	Link da documentação
AWS Elastic Disaster Recovery	O que é o Elastic Disaster Recovery
AWS Backup	O que é AWS Backup
Controlador de recuperação de aplicativos Amazon (ARC) (ARC)	O que é o Amazon Application Recovery Controller (ARC)

Tópicos

AWS Resilience Hub — Gestão da resiliência

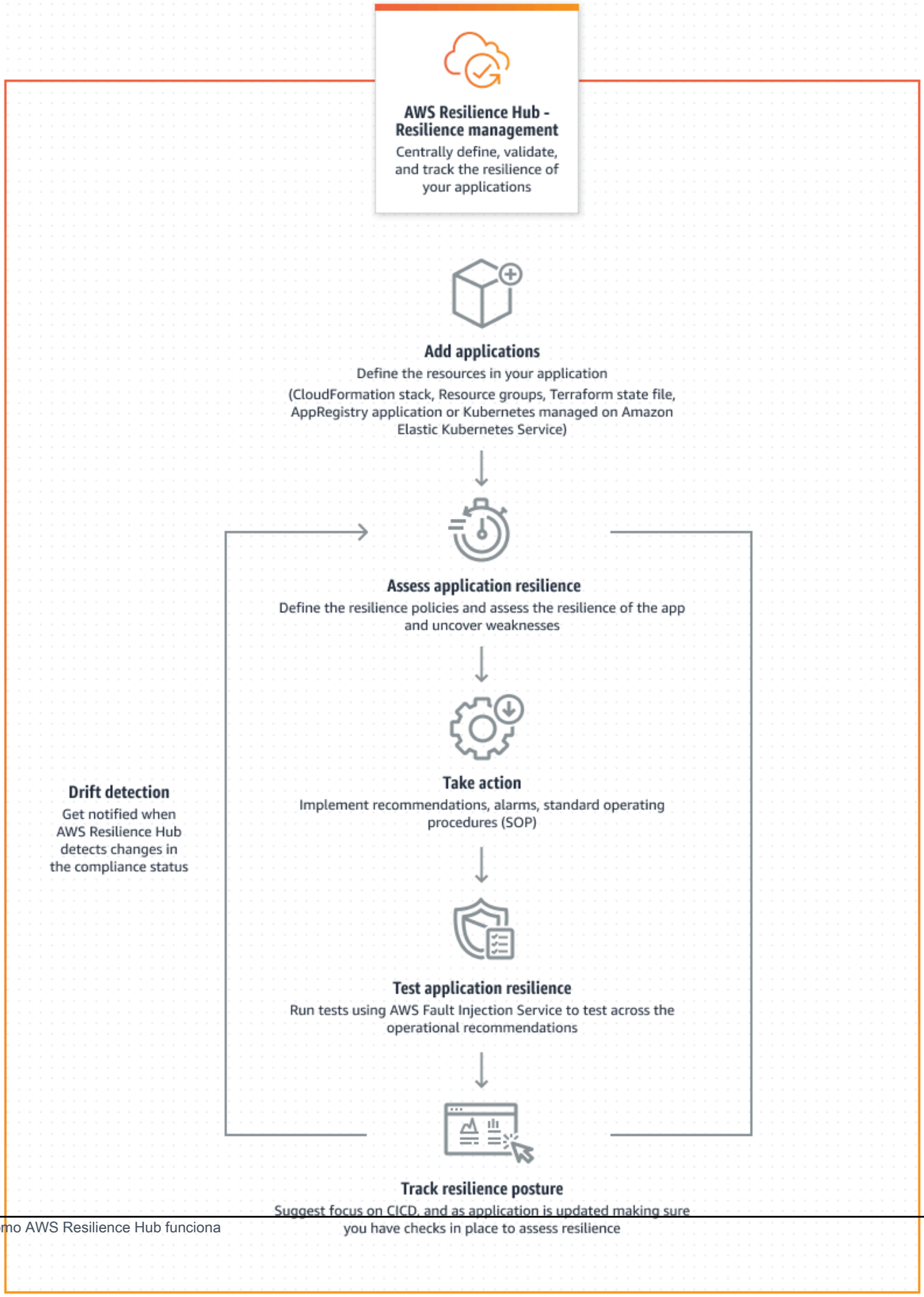
AWS Resilience Hub oferece um local central para definir, validar e rastrear a resiliência do seu AWS aplicativo. AWS Resilience Hub ajuda você a proteger seus aplicativos contra interrupções e a reduzir os custos de recuperação para otimizar a continuidade dos negócios e ajudar a atender aos requisitos regulatórios e de conformidade. Você pode usar AWS Resilience Hub para fazer o seguinte:

- Analisar sua infraestrutura e obter recomendações para melhorar a resiliência de seus aplicativos. Além da orientação arquitetônica para melhorar a resiliência de seu aplicativo, as recomendações fornecem código para atender à sua política de resiliência, implementando testes, alarmes e procedimentos operacionais padrão (SOPs) que você pode implantar e executar com seu aplicativo em seu pipeline de integração e entrega (CI/CD).
- Avalie as metas do objetivo do tempo de recuperação (RTO) e do objetivo do ponto de recuperação (RPO) sob diferentes condições.
- Otimizar a continuidade dos negócios e reduzir os custos de recuperação.
- Identificar e resolver problemas antes que eles ocorram na produção.

Depois de implantar um aplicativo na produção, você pode adicioná-lo AWS Resilience Hub ao seu pipeline de CI/CD para validar cada compilação antes que ela seja lançada em produção.

Como AWS Resilience Hub funciona

O diagrama a seguir fornece um resumo de alto nível de como funciona AWS Resilience Hub .


AWS Resilience Hub - Resilience management
Centrally define, validate, and track the resilience of your applications
Add applications
Define the resources in your application
(CloudFormation stack, Resource groups, Terraform state file, AppRegistry application or Kubernetes managed on Amazon Elastic Kubernetes Service)
Assess application resilience
Define the resilience policies and assess the resilience of the app and uncover weaknesses
Take action
Implement recommendations, alarms, standard operating procedures (SOP)
Test application resilience
Run tests using AWS Fault Injection Service to test across the operational recommendations
Track resilience posture
Suggest focus on CICD, and as application is updated making sure you have checks in place to assess resilience
Drift detection
Get notified when AWS Resilience Hub detects changes in the compliance status

Descrever

Descreva seu aplicativo importando recursos de AWS CloudFormation pilhas, AWS Resource Groups arquivos de estado do Terraform e clusters do Amazon Elastic Kubernetes Service, ou você pode escolher entre aplicativos que já estão definidos em. AWS Service Catalog AppRegistry

Definir

Defina as políticas de resiliência para seus aplicativos. Essas políticas incluem RTO e RPO visam interrupções em aplicativos, infraestrutura, zona de disponibilidade e região. Essas metas são usadas para estimar se o aplicativo atende à política de resiliência.

Avaliar

Depois de descrever seu aplicativo e anexar uma política de resiliência a ele, execute uma avaliação de resiliência. A AWS Resilience Hub avaliação usa as melhores práticas do AWS Well-Architected Framework para analisar os componentes de um aplicativo e descobrir possíveis pontos fracos de resiliência. Esses pontos fracos podem ser causados por configuração incompleta da infraestrutura, configuração incorreta ou situações em que melhorias adicionais na configuração são necessárias. Para melhorar a resiliência, atualize seu aplicativo e sua política de resiliência de acordo com as recomendações do relatório de avaliação. As recomendações incluem configurações de componentes, alarmes, testes e recuperação. SOPs Em seguida, você pode executar outra avaliação e comparar os resultados com o relatório anterior para ver o quanto a resiliência melhora. Reitere esse processo até que sua carga de trabalho estimada RTO e sua carga de trabalho estimada atinjam RPO suas RTO metas. RPO

Validar

Execute testes para medir a resiliência de seus AWS recursos e o tempo necessário para se recuperar de aplicativos, infraestrutura, zona de disponibilidade e Região da AWS incidentes. Para medir a resiliência, esses testes simulam interrupções de seus recursos. AWS Exemplos de interrupções incluem erros indisponíveis na rede, failovers, processos interrompidos, recuperação de RDS inicialização da Amazon e problemas com sua zona de disponibilidade.

Visualizar e monitorar

Depois de implantar um AWS aplicativo na produção, você pode usá-lo AWS Resilience Hub para continuar monitorando a postura de resiliência do aplicativo. Se ocorrer uma interrupção, o operador poderá visualizar a interrupção AWS Resilience Hub e iniciar o processo de recuperação associado.

AWS Resilience Hub — Teste de resiliência

AWS Resilience Hub permite que você realize testes e experimentos do Amazon Fault Injection Service (AWS FIS) em suas AWS cargas de trabalho e mantenha a resiliência ideal. Esses testes estressam um aplicativo criando eventos disruptivos para que você possa observar como seu aplicativo responde. AWS FIS fornece vários cenários pré-criados e uma grande seleção de ações que geram interrupções. Além disso, também inclui controles e barreiras de proteção necessários para executar os experimentos em produção. Os controles e barreiras de proteção incluem opções para realizar a reversão automática ou interromper o experimento se condições específicas forem atendidas. Para começar a usar o AWS FIS para executar experimentos no AWS Resilience Hub console, preencha os pré-requisitos definidos na seção. the section called “Pré-requisitos”

A tabela a seguir lista todas as AWS FIS opções disponíveis no painel de navegação e os links para a AWS FIS documentação associada que contém os procedimentos para começar a usar os AWS FIS testes do AWS Resilience Hub console.

AWS FIS opções e referências do menu de navegação

AWS FIS opção de menu de navegação	AWS FIS documentação
Teste de resiliência	Criar um modelo de experimento
Biblioteca de cenários	AWS FIS biblioteca
Modelos de experimentos	Modelos de experimentos para AWS FIS

A tabela a seguir lista todas as AWS FIS opções disponíveis no menu suspenso na seção Teste de resiliência e os links para a AWS FIS documentação associada que contém os procedimentos para começar a usar os AWS FIS testes no console. AWS Resilience Hub

AWS FIS opções e referências do menu suspenso

AWS FIS opção de menu suspenso	AWS FIS documentação
Criar modelo de experimento	Criar um modelo de experimento
Criar um experimento a partir do cenário	Usar um cenário

AWS Resilience Hub conceitos

Esses conceitos podem ajudar você a entender melhor a abordagem da AWS Resilience Hub da para ajudar a melhorar a resiliência do aplicativo e evitar interrupções no aplicativo.

Resiliência

A capacidade de manter a disponibilidade e se recuperar de interrupções operacionais e de software em um período de tempo designado.

Objetivo do ponto de recuperação (RPO)

O máximo período de tempo aceitável desde o último ponto de recuperação de dados. Isso determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

Objetivo de tempo de recuperação (RTO)

Atraso aceitável máximo entre a interrupção e a restauração do serviço. Determina o que é considerado uma janela de tempo aceitável quando o serviço não está disponível.

Objetivo estimado do tempo de recuperação da workload

O objetivo estimado do tempo de recuperação da carga de trabalho (carga de trabalho estimadaRTO) é o RTO que seu aplicativo deve atingir com base na definição do aplicativo importado e, em seguida, executar uma avaliação.

Objetivo de ponto de recuperação estimado da workload

O objetivo estimado do ponto de recuperação da carga de trabalho (carga de trabalho estimadaRPO) é o RPO que seu aplicativo deve atingir com base na definição do aplicativo importado e, em seguida, executar uma avaliação.

Aplicativo

Um AWS Resilience Hub aplicativo é uma coleção de recursos AWS suportados que são continuamente monitorados e avaliados para gerenciar sua postura de resiliência.

Componente do aplicativo

Um grupo de AWS recursos relacionados que funcionam e falham como uma única unidade. Por exemplo, se você tiver um banco de dados primário e de réplica, os dois bancos de dados pertencerão ao mesmo componente de aplicativo (AppComponent).

AWS Resilience Hub determina quais AWS recursos podem pertencer a qual tipo de AppComponent. Por exemplo, um `DBInstance` pode pertencer a `AWS::ResilienceHub::DatabaseAppComponent`, mas não a `AWS::ResilienceHub::ComputeAppComponent`.

Status de conformidade do aplicativo

AWS Resilience Hub relata os seguintes tipos de status de conformidade para seus aplicativos.

Política cumprida

Estima-se que o aplicativo atinja suas RPO metas RTO e metas definidas na política. Todos os seus componentes atendem aos objetivos da política definida. Por exemplo, você selecionou uma RPO meta RTO de 24 horas para interrupções em todas as AWS regiões. AWS Resilience Hub pode ver que seus backups são copiados para sua região alternativa. Ainda se espera que você mantenha uma recuperação de um procedimento operacional padrão de backup (SOP) e que a teste e cronometre. Isso está nas recomendações operacionais e faz parte de sua pontuação geral de resiliência.

Política violada

Não foi possível estimar que o RTO aplicativo atendesse às RPO metas definidas na política. Um ou mais deles não satisfazem os objetivos políticos. AppComponents Por exemplo, você selecionou uma RTO RPO meta de 24 horas para interrupções em todas as AWS regiões, mas a configuração do seu banco de dados não inclui nenhum método de recuperação entre regiões, como replicação global e cópias de backup.

Não avaliado

O aplicativo requer uma avaliação. Atualmente, não é avaliado ou monitorado.

Alterações detectadas

Há uma nova versão publicada do aplicativo que ainda não foi avaliada.

Detecção de desvios

AWS Resilience Hub executa uma notificação de deriva enquanto executa uma avaliação do seu aplicativo para verificar se as alterações nas AppComponent configurações afetaram o status de conformidade do seu aplicativo. Além disso, ele também verifica e detecta alterações, como adição ou exclusão de recursos nas fontes de entrada do aplicativo, e notifica sobre as mesmas. Para comparação, AWS Resilience Hub usa a avaliação anterior na qual o componente do aplicativo atendeu à política. AWS Resilience Hub detecta os seguintes tipos de desvios:

- Desvio da política de aplicação — Esse tipo de desvio identifica todos os AppComponents que estavam em conformidade com a política na avaliação anterior, mas não cumpriram na avaliação atual.
- Desvio de recursos do aplicativo — Esse tipo de desvio identifica todos os recursos desviados na versão atual do aplicativo.

Avaliação de resiliência

AWS Resilience Hub usa uma lista de lacunas e possíveis soluções para medir a eficácia de uma política selecionada para se recuperar e continuar após um desastre. Ele avalia cada componente do aplicativo ou o status de conformidade do aplicativo com a política. Esse relatório inclui recomendações de otimização de custos e referências a possíveis problemas.

Pontuações de resiliência

AWS Resilience Hub gera uma pontuação que indica até que ponto seu aplicativo segue nossas recomendações para atender à política de resiliência, aos alarmes, aos procedimentos operacionais padrão (SOPs) e aos testes do aplicativo.

Tipo de interrupção

AWS Resilience Hub ajuda você a avaliar a resiliência contra os seguintes tipos de interrupções:

Aplicativo

A infraestrutura está íntegra, mas a pilha de aplicativos ou software não opera conforme necessário. Isso pode ocorrer após a implantação de um novo código, alterações na configuração, corrupção de dados ou mau funcionamento das dependências downstream.

Infraestrutura de nuvem

A infraestrutura de nuvem não está funcionando conforme o esperado devido a uma interrupção. Pode ocorrer uma interrupção devido a um erro local em um ou mais componentes. Na maioria dos casos, esse tipo de interrupção é resolvido reinicializando, reciclando ou recarregando os componentes defeituosos.

Interrupção de AZ da infraestrutura de nuvem

Uma ou mais zonas de disponibilidade não estão disponíveis. Esse tipo de interrupção pode ser resolvido com a mudança para uma zona de disponibilidade diferente.

Incidente na região de infraestrutura de nuvem

Uma ou mais regiões não estão disponíveis. Esse tipo de incidente pode ser resolvido mudando para uma Região da AWS diferente.

Experimentos de injeção de falhas

AWS Resilience Hub recomenda testes para verificar a resiliência do aplicativo contra diferentes tipos de interrupções. Essas interrupções incluem aplicativos, infraestrutura, zonas de disponibilidade (AZ) ou incidentes de Região da AWS de componentes de aplicativos.

Esses experimentos permitem que você faça o seguinte:

- Injete uma falha.
- Verifique se os alarmes podem detectar uma interrupção.
- Verifique se os procedimentos de recuperação, ou procedimentos operacionais padrão (SOPs), funcionam corretamente para recuperar o aplicativo da interrupção.

Testes para SOPs medir a carga de trabalho estimada RTO e a carga de trabalho RPO estimada. Você pode testar diferentes configurações de aplicativos e medir se a saída RTO RPO atende aos objetivos definidos em sua política.

SOP

Um procedimento operacional padrão (SOP) é um conjunto prescritivo de etapas projetado para recuperar seu aplicativo de forma eficiente em caso de interrupção ou alarme. Com base na

avaliação do aplicativo, AWS Resilience Hub recomenda um conjunto de SOPs e é recomendável preparar, testar e medir antes SOPs de uma interrupção para garantir a recuperação oportuna.

AWS Resilience Hub personas

A criação de um aplicativo corporativo exige um esforço colaborativo de diferentes equipes multifuncionais, como infraestrutura, continuidade de negócios, proprietário do aplicativo e outras partes interessadas responsáveis pelo monitoramento dos aplicativos. As diferentes personas de diferentes equipes contribuem para a criação e gerenciamento de aplicativos AWS Resilience Hub, cada uma com uma função e responsabilidades diferentes. Para saber mais sobre como conceder permissões a diferentes personas, consulte. the section called “AWS Resilience Hub referência de personas e IAM permissões”

Para começar a criar aplicativos e executar avaliações no AWS Resilience Hub, recomendamos que você crie as seguintes personas:

- Gerente de aplicativos de infraestrutura — Os usuários com essa personalidade são responsáveis por instalar, configurar e manter os recursos de infraestrutura e aplicativos, garantindo a confiabilidade e a segurança do aplicativo. Suas responsabilidades incluem o seguinte:
  - Garantir que os aplicativos sejam implantados e atualizados regularmente
  - Monitorando o desempenho do sistema
  - Solução de problemas
  - Implementando planos de backup e recuperação de desastres
- Gerente de continuidade de negócios — os usuários com essa personalidade são responsáveis por ditar as políticas de aplicativos e determinar a importância comercial dos aplicativos. Suas responsabilidades incluem o seguinte:
  - Tomando decisões importantes na definição de políticas
  - Avaliando a importância dos negócios
  - Alocação de recursos para aplicativos críticos
  - Avaliação e gerenciamento de riscos
- Proprietário do aplicativo — Os usuários com essa persona são responsáveis por garantir aplicativos altamente disponíveis e confiáveis. Suas responsabilidades incluem o seguinte:
  - Definindo identificadores-chave de desempenho para medir e monitorar o desempenho do aplicativo e identificar gargalos
  - Organizando treinamentos para várias partes interessadas

- Garantir que a seguinte documentação seja up-to-date:
  - Arquitetura da aplicação
  - Processos de implantação
  - Configurações de monitoramento
  - Técnicas de otimização de desempenho
- Acesso somente para leitura — Os usuários com essa persona estão restritos às permissões somente para leitura. Suas responsabilidades incluem manter a visibilidade e a supervisão do desempenho e da integridade de um aplicativo monitorando a pontuação de resiliência, as recomendações operacionais e as recomendações de resiliência. Além disso, eles também são responsáveis por identificar problemas, tendências e áreas de melhoria para garantir que o aplicativo atenda aos objetivos da organização.

AWS Resilience Hub recursos suportados

Os recursos que afetam o desempenho do aplicativo em caso de interrupção são totalmente suportados por recursos AWS Resilience Hub de alto nível, como e. `AWS::RDS::DBInstance` `AWS::RDS::DBCluster`

Para saber mais sobre as permissões necessárias AWS Resilience Hub para incluir recursos de todos os serviços suportados em sua avaliação, consultethe section called "AWSResilienceHubAsssessmentExecutionPolicy".

AWS Resilience Hub oferece suporte a recursos dos seguintes AWS serviços:

- Computação
  - Nuvem de computação elástica da Amazon (AmazonEC2)

> **Note**
>
> AWS Resilience Hub não suporta o formato antigo Amazon Resource Name (ARN) para acessar EC2 os recursos da Amazon. O novo ARN formato usa o ID da sua AWS conta e permite a capacidade aprimorada de marcar recursos em seu cluster, além de monitorar o custo dos serviços e tarefas executados em seu cluster.
>
> - Formato antigo (obsoleto) — `arn:aws:ec2:<region>::instance/<instance-id>`

- Novo formato — `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`

Para obter mais informações sobre o novo ARN formato, consulte Migrando sua ECS implantação da Amazon para o novo formato ARN e o formato de ID de recurso.

  - AWS Lambda
  - Amazon Elastic Kubernetes Service (Amazon) EKS
  - Amazon Elastic Container Service (AmazonECS)
  - AWS Step Functions
- Banco de dados
  - Amazon Relational Database Service (AmazonRDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
- Rede e entrega de conteúdo
  - Amazon Route 53
  - Elastic Load Balancing
  - Tradução de endereços de rede (NAT)
- Armazenamento
  - Amazon Elastic Block Store (AmazonEBS)
  - Amazon Elastic File System (AmazonEFS)
  - Amazon Simple Storage Service (Amazon S3)
  - Servidor FSx de arquivos Amazon para Windows
- Outros
  - Amazon API Gateway
  - Controlador de recuperação de aplicativos da Amazon (ARC) (AmazonARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS Recuperação flexível de desastres

Note

- AWS Resilience Hub fornece transparência adicional aos recursos do seu aplicativo, permitindo que você visualize as instâncias suportadas de cada recurso. Além disso, AWS Resilience Hub fornece recomendações de resiliência mais precisas identificando uma instância exclusiva de cada recurso e descobrindo as instâncias do recurso durante o processo de avaliação. Para obter mais informações sobre como adicionar instâncias de recursos ao aplicativo, consulteEditando recursos AWS Resilience Hub do aplicativo.
- AWS Resilience Hub suporta Amazon EKS e Amazon ECS on AWS Fargate.
- AWS Resilience Hub apoia a avaliação de AWS Backup recursos como parte dos seguintes serviços:
  - Amazon EBS
  - Amazon EFS
  - Amazon S3
  - Amazon Aurora Global Database
  - Amazon DynamoDB
  - RDSServiços da Amazon
  - Servidor FSx de arquivos Amazon para Windows
- A Amazon ARC AWS Resilience Hub avalia somente o Amazon DynamoDB global, o Elastic Load Balancing, o Amazon e os grupos. RDS AWS Auto Scaling
- AWS Resilience Hub Para avaliar os recursos entre regiões, agrupe os recursos em um único componente de aplicativo. Para obter mais informações sobre os recursos com suporte para cada um dos componentes do aplicativo e recursos de agrupamento do AWS Resilience Hub , consulte Agrupando recursos em um componente de aplicativo.
- Atualmente, AWS Resilience Hub não oferece suporte a avaliações entre regiões para EKS clusters da Amazon se o EKS cluster da Amazon estiver localizado ou se o aplicativo for criado em uma região habilitada para opt-in. AWS
- Atualmente, AWS Resilience Hub avalia somente os seguintes tipos de recursos do Kubernetes:
  - Implantações
  - ReplicaSets
  - Pods

AWS Resilience Hub ignora os seguintes tipos de recursos:

- Recursos que não afetam a carga de trabalho estimada RTO ou a carga de trabalho estimada RPO — Recursos como**`AWS::RDS::DBParameterGroup`**, que não afetam a carga de trabalho estimada RTO ou a carga de trabalho estimadaRPO, são ignorados por. AWS Resilience Hub
- Recursos de nível não superior — importa AWS Resilience Hub somente recursos de nível superior, porque eles podem derivar outras propriedades consultando as propriedades dos recursos de nível superior. Por exemplo, `AWS::ApiGateway::RestApi` e `AWS::ApiGatewayV2::Api` são recursos compatíveis com o Amazon API Gateway. No entanto, `AWS::ApiGatewayV2::Stage` não é um recurso de alto nível. Portanto, ele não é importado por AWS Resilience Hub.

> **Note**
>
> Recursos não compatíveis
>
> - Você não pode identificar vários recursos usando AWS Resource Groups (Amazon Route 53 RecordSets e API -GWHTTP) e recursos globais do Amazon Aurora. Se quiser analisar esses recursos como parte de sua avaliação, você deve adicionar manualmente o recurso ao aplicativo. No entanto, quando você adiciona recursos globais do Amazon Aurora para avaliação, eles devem ser agrupados com o componente de aplicativo da RDS instância da Amazon. Para obter mais informações sobre recursos de edição, consulte the section called “Editar recursos de aplicativo”.
> - Esses recursos podem afetar a recuperação de aplicativos, mas eles não são totalmente suportados AWS Resilience Hub no momento. AWS Resilience Hub faz um esforço para avisar os usuários sobre recursos não suportados se o aplicativo for apoiado por uma AWS CloudFormation pilha, arquivo de estado do Terraform ou aplicativo. AWS Resource Groups AppRegistry

Conceitos básicos

Esta seção descreve como começar a usar AWS Resilience Hub. Isso inclui a criação de permissões do AWS Identity and Access Management (IAM) para uma conta.

Tópicos

Pré-requisitos

Antes de usar o AWS Resilience Hub, você deve preencher os seguintes pré-requisitos:

- AWS contas — Crie uma ou mais AWS contas para cada tipo de conta (contas primárias/secundárias/de recursos) que você deseja usar. AWS Resilience Hub Para obter mais informações sobre como criar e gerenciar AWS contas, consulte o seguinte:
  - AWS Usuário iniciante — Introdução: Você é um AWS usuário iniciante?
  - Gerenciando AWS conta — https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management Permissões (IAM) — Depois de criar as AWS contas, você deve configurar as funções necessárias e as permissões do IAM para cada uma das contas que você criou. Por exemplo, se você criou uma AWS conta para acessar os recursos do aplicativo, deverá configurar uma nova função e configurar as permissões necessárias do IAM AWS Resilience Hub para acessar os recursos do aplicativo a partir da sua conta. Para saber mais sobre as permissões do IAM, consulte the section called “Como o AWS Resilience Hub funciona com IAM” e para obter mais informações sobre como adicionar uma política ao perfil, consulte the section called “Definindo a política de confiança usando o JSON arquivo”.

  Para começar rapidamente a adicionar permissões do IAM a usuários, grupos e funções, você pode usar nossas políticas AWS gerenciadas (the section called “AWS políticas gerenciadas”). É mais fácil usar políticas AWS gerenciadas para cobrir casos de uso comuns que estão disponíveis em você Conta da AWS do que escrever políticas você mesmo. AWS Resilience Hub adiciona permissões adicionais a uma política AWS gerenciada para estender o suporte a outros AWS serviços e incluir novos recursos. Dessa forma:

- Se você já é um cliente e deseja que seu aplicativo use as melhorias mais recentes em sua avaliação, você deve publicar uma nova versão do aplicativo e, então, executar uma nova avaliação. Para obter mais informações, consulte os tópicos a seguir.
  - the section called “Publicar uma nova versão do aplicativo”
  - the section called “Executar avaliações de resiliência”
- Se você não estiver usando políticas AWS gerenciadas para atribuir permissões apropriadas do IAM a usuários, grupos e funções, deverá configurar essas permissões manualmente. Para obter mais informações sobre políticas AWS gerenciadas, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Adicionar um aplicativo ao AWS Resilience Hub

AWS Resilience Hub oferece avaliação e validação de resiliência que se integram ao seu ciclo de vida de desenvolvimento de software. AWS Resilience Hub ajuda você a preparar e proteger proativamente seus AWS aplicativos contra interrupções ao:

- Descobrir os pontos fracos de resiliência.
- Estimar se o objetivo de tempo de recuperação (RTO) e o objetivo de ponto de recuperação (RPO) podem ser atingidos.
- Resolver problemas antes que eles sejam lançados em produção.

Esta seção vai guiá-lo sobre como adicionar um aplicativo. Você reúne recursos de um aplicativo existente, AWS CloudFormation pilhas ou cria uma AppRegistry política de resiliência apropriada. AWS Resource Groups Depois de descrever um aplicativo, você pode publicá-lo e gerar um relatório de avaliação sobre a resiliência do seu aplicativo. AWS Resilience Hub Em seguida, você pode usar as recomendações da avaliação para melhorar a resiliência. Você pode executar outra avaliação, comparar os resultados e, em seguida, iterar até que a carga de trabalho estimada RTO e a carga de trabalho estimada RPO atinjam suas metas. RTO RPO

Tópicos

Etapa 1: comece adicionando uma aplicativo

Comece AWS Resilience Hub descrevendo os detalhes do seu AWS aplicativo e executando um relatório para avaliar a resiliência.

Para começar, na página AWS Resilience Hub inicial, em Começar, escolha Adicionar aplicativo.

Para saber mais sobre os custos e o faturamento associados a AWS Resilience Hub, consulte AWS Resilience Hub preços.

Descreva os detalhes do seu aplicativo no AWS Resilience Hub

Esta seção mostra como descrever os detalhes do seu AWS aplicativo existente em AWS Resilience Hub.

Descrever os detalhes da seu aplicativo

1. Insira um nome para o aplicativo.
2. (Opcional) Insira uma descrição para o aplicativo.

Próximo

Etapa 2: como seu aplicativo é gerenciado?

Etapa 2: como seu aplicativo é gerenciado?

Além de AWS CloudFormation pilhas AWS Resource Groups, AppRegistry aplicativos e arquivos de estado do Terraform, você pode adicionar recursos que estão localizados nos clusters do Amazon Elastic Kubernetes Service (Amazon). EKS Ou seja, o AWS Resilience Hub permite que você

adicione recursos que estão localizados em seus EKS clusters da Amazon como recursos opcionais. Esta seção fornece as seguintes opções, que ajudam você a determinar a localização dos recursos do seu aplicativo.

- Coleções de recursos: selecione essa opção se quiser descobrir recursos de uma das coleções de recursos. As coleções de recursos incluem AWS CloudFormation pilhas AWS Resource Groups, AppRegistry aplicativos e arquivos de estado do Terraform.

  Se selecionar esta opção, você deve realizar um dos procedimentos no the section called "Adicionar coleções de recursos".
- EKSsomente — Selecione essa opção se quiser descobrir recursos de namespaces dentro dos clusters da AmazonEKS.

  Se selecionar esta opção, você deve realizar o procedimento no the section called "Adicionar EKS clusters"
- Coleções de recursos e EKS — Selecione essa opção se quiser descobrir recursos de uma das coleções de recursos e EKS clusters da Amazon.

  Se selecionar esta opção, realize um dos procedimentos no the section called "Adicionar coleções de recursos" e, em seguida, conclua o procedimento no the section called "Adicionar EKS clusters".

> **Note**
>
> Para obter informações sobre o número de recursos suportados por aplicativo, consulte Service Quotas.

Próximo

Etapa 3: adicionar recursos ao seu AWS Resilience Hub aplicativo

Etapa 3: adicionar recursos ao seu AWS Resilience Hub aplicativo

Esta seção discute as seguintes opções que você pode usar para formar a base da estrutura do seu aplicativo:

- the section called "Adicionar coleções de recursos"

- the section called “Adicionar EKS clusters”

Adicionar coleções de recursos

Esta seção discute os seguintes métodos que você usa para formar a base da estrutura do seu aplicativo:

- Usando AWS CloudFormation pilhas
- Usando AWS Resource Groups
- Usando AppRegistry aplicativos
- Usar arquivos de estado do Terraform
- Usando um AWS Resilience Hub aplicativo existente

Usando AWS CloudFormation pilhas

Escolha as AWS CloudFormation pilhas que contêm os recursos que você deseja usar no aplicativo que você está descrevendo. As pilhas podem ser das Conta da AWS que você está usando para descrever o aplicativo ou podem ser de contas ou regiões diferentes.

Para descobrir os recursos que formam a base da estrutura de seu aplicativo

1. Selecione CloudFormation pilhas para descobrir seus recursos baseados em pilhas.
2. Escolha pilhas na lista suspensa Selecionar pilhas associadas à sua região. Conta da AWS

   Para usar pilhas que estão em uma região diferente Conta da AWS ou em ambas, insira o Amazon Resource Name (ARN) da pilha na caixa Adicionar pilha fora da AWS região e escolha Adicionar pilha. ARN Para obter mais informações sobreARNs, consulte Amazon Resource Names (ARNs) na Referência AWS geral.

Usando AWS Resource Groups

Escolha o AWS Resource Groups que contém os recursos que você deseja usar no aplicativo que você está descrevendo.

Para descobrir os recursos que formam a base da estrutura de seu aplicativo

1. Selecione Grupos de recursos para descobrir os AWS Resource Groups que contêm os recursos.

2. Escolha recursos na lista suspensa Selecionar grupos de recursos.

   Para usar AWS Resource Groups que estejam em uma região diferente Conta da AWS ou em ambas, insira o Amazon Resource Name (ARN) da pilha na ARN caixa Resource Group e escolha Add Resource Group ARN. Para obter mais informações sobreARNs, consulte Amazon Resource Names (ARNs) na Referência AWS geral.

Usando AppRegistry aplicativos

Você pode adicionar somente um AppRegistry aplicativo por vez.

Escolha os AppRegistry aplicativos que contêm os recursos que você deseja usar no aplicativo que você está descrevendo.

Para descobrir os recursos que formam a base da estrutura de seu aplicativo

1. Selecione AppRegistrypara selecionar em uma lista de aplicativos criados em AppRegistry.
2. Escolha os aplicativos que foram criados em AppRegistry, na lista suspensa Selecionar aplicativo. Você só pode escolher um aplicativo por vez.

Usar arquivos de estado do Terraform

Escolha o arquivo de estado do Terraform que contém os recursos do bucket do S3 que deseja usar no aplicativo que você está descrevendo. Você pode navegar até o local do seu arquivo de estado do Terraform ou fornecer um link para um arquivo de estado do Terraform ao qual você tenha acesso e que esteja localizado em uma região diferente.

> **Note**
>
> AWS Resilience Hub suporta a versão do arquivo de estado do Terraform `0.12` e versões posteriores.

Para descobrir os recursos que formam a base da estrutura de seu aplicativo

1. Selecione os Arquivos de estado do Terraform para descobrir seus recursos de bucket do S3.
2. Na seção Selecionar arquivos de estado, escolha Procurar no S3 para navegar até o local do seu arquivo de estado do Terraform.

Para usar arquivos de estado do Terraform localizados em uma região diferente, forneça o link para a localização do arquivo de estado do Terraform no URL campo S3 e escolha Adicionar S3. URL

O limite para arquivos de estado do Terraform é de 4 megabytes (MB).

3. Selecione seu bucket do S3 na seção Buckets.
4. Na seção Objetos, selecione uma chave e selecione Escolher.

Usando um AWS Resilience Hub aplicativo existente

Para começar, use um aplicativo existente.

Para descobrir os recursos que formam a base da estrutura de seu aplicativo

1. Selecione Aplicativo existente para criar seu aplicativo a partir de um aplicativo existente.
2. Selecione um aplicativo na lista suspensa Selecionar aplicativo existente.

Adicionar EKS clusters

Esta seção discute sobre o uso de EKS clusters da Amazon para formar a base da estrutura do seu aplicativo.

> **Note**
>
> Você deve ter EKS permissões e IAM funções adicionais da Amazon para se conectar ao EKS cluster da Amazon. Para obter mais informações sobre como adicionar EKS permissões da Amazon com uma única conta e entre contas e IAM funções adicionais para se conectar ao cluster, consulte os seguintes tópicos:
>
> - AWS Resilience Hub referência de permissões de acesso
> - the section called “Habilitando o AWS Resilience Hub acesso ao seu EKS cluster da Amazon”

Escolha os EKS clusters e namespaces da Amazon que contêm os recursos que você deseja usar no aplicativo que você está descrevendo. Os EKS clusters da Amazon podem ser dos Conta da AWS

que você está usando para descrever o aplicativo ou podem ser de contas diferentes ou regiões diferentes.

> **Note**
>
> AWS Resilience Hub Para avaliar seus EKS clusters da Amazon, você deve adicionar manualmente os namespaces relevantes a cada um dos clusters da Amazon na seção de EKS EKSclusters e namespaces. O nome do namespace deve corresponder exatamente ao nome do namespace em seus clusters da Amazon. EKS

Para adicionar EKS clusters da Amazon

1. Escolha os EKS clusters da Amazon na lista suspensa Escolher EKS clusters que estão associados à sua região Conta da AWS .
2. Para usar EKS clusters da Amazon que estão em uma região diferente ou em ambas, insira o Amazon Resource Name (ARN) da pilha na caixa Cross account ou Region e escolha Add EKS ARN. Conta da AWS Para obter mais informações sobreARNs, consulte Amazon Resource Names (ARNs) na Referência AWS geral.

   Para obter mais informações sobre a adição de permissões para acessar clusters entre regiões do Amazon Elastic Kubernetes Service, consulte the section called “Habilitando o AWS Resilience Hub acesso ao seu EKS cluster da Amazon”.

Para adicionar namespaces dos clusters selecionados da Amazon EKS

1. Na seção Adicionar namespaces, na tabela de EKSclusters e namespaces, selecione o botão de opção localizado à esquerda do nome do EKS cluster da Amazon e escolha Atualizar namespaces.

   Você pode identificar os EKS clusters da Amazon da seguinte forma:

   - EKSnome do cluster — Indica o nome dos EKS clusters selecionados da Amazon.
   - Nº de namespaces — Indica o número de namespaces selecionados nos clusters da Amazon. EKS
   - Status — Indica se AWS Resilience Hub incluiu os namespaces dos EKS clusters selecionados da Amazon em seu aplicativo. Você pode identificar o status usando as seguintes opções:

- Namespace obrigatório — Indica que você não incluiu nenhum namespace do cluster da Amazon. EKS
- Namespaces adicionados — Indica que você incluiu um ou mais namespaces do cluster da Amazon. EKS

2. Para adicionar um namespace, na caixa de diálogo Atualizar namespaces, escolha Adicionar um novo namespace.

   A caixa de diálogo Atualizar namespaces exibe todos os namespaces que você selecionou do seu EKS cluster da Amazon, como uma opção editável.

3. Na caixa de diálogo Atualizar namespaces, você tem as seguintes opções de edição:

   - Para adicionar um novo namespace, escolha Adicionar um novo namespace e, em seguida, insira o nome do namespace na caixa namespace.

     O nome do namespace deve corresponder exatamente ao nome do namespace no seu cluster da Amazon. EKS
   - Para remover um namespace, escolha Remover localizado ao lado do namespace.
   - Para aplicar os namespaces selecionados a todos os EKS clusters da Amazon, escolha Aplicar namespaces a todos os clusters. EKS

     Se você escolher essa opção, sua seleção anterior de namespace nos outros EKS clusters da Amazon será substituída pela seleção de namespace atual.

4. Para incluir os namespaces atualizados em seu aplicativo, escolha Atualizar.

Próximo

Etapa 4: definir RTO e RPO

Etapa 4: definir RTO e RPO

Você pode definir uma nova política de resiliência com suas próprias RTO RPO /metas ou escolher uma política de resiliência existente com /metas predefinidasRTO. RPO Caso queira usar uma das políticas de resiliência existentes, selecione a opção Escolher uma política existente e selecione um aplicativo de destino existente na lista suspensa Item de opção.

Para definir suas próprias RTO RPO /metas

1. Selecione a opção Criar uma nova política de resiliência.

2. Insira um nome para a política de resiliência.
3. (Opcional) Insira uma descrição para a política de resiliência.
4. Defina seu RTO RTO/RPOna seção RPO /targets.

> **Note**
>
> - Preenchemos um padrão RTO e RPO para seu aplicativo. Você pode alterar o RTO e RPO agora ou depois de avaliar o aplicativo.
> - AWS Resilience Hub permite que você insira um valor zero nos RPOcampos RTOe da sua política de resiliência. Mas, ao avaliar seu aplicativo, o menor resultado de avaliação possível é próximo de zero. Portanto, se você inserir um valor zero nos RPOcampos RTOe, a carga de trabalho estimada RTO e RPO os resultados estimados da carga de trabalho serão próximos de zero e o status de conformidade do seu aplicativo será definido como Política violada.

5. Para definirRTO/RPOpara sua infraestrutura e AZ, escolha a seta para a direita para expandir a RPO seção Infraestrutura RTO e.
6. Em RTORPO/targets, insira um valor numérico na caixa e escolha a unidade de tempo que o valor representa para RTOe. RPO

   Repita essas entradas para Infraestrutura e Zona de Disponibilidade na RPO seção Infraestrutura RTO e.
7. (Opcional) Se você tiver um aplicativo multirregional e quiser definir uma região RTO eRPO, ative Região - Opcional.

   Em RTOe RPO, insira um valor numérico na caixa e escolha a unidade de tempo que o valor representa para RTOe. RPO

Próximo

the section called “Etapa 5: configurar a avaliação programada e a notificação de deriva”

Etapa 5: configurar avaliações agendadas e notificação de deriva

AWS Resilience Hub permite que você configure avaliações programadas e notificações de desvio para avaliar seu aplicativo diariamente e ser notificado quando um desvio for detectado.

Para configurar a notificação de desvio

1. Para avaliar sua inscrição diariamente, ative Avaliar automaticamente diariamente.

   Se esta opção estiver ativada, o cronograma de avaliação diária começará somente após:

   - O aplicativo ser avaliado manualmente com sucesso pela primeira vez.
   - O aplicativo está configurado com uma IAM função apropriada.
   - Se seu aplicativo estiver configurado com as permissões de IAM usuário atuais, você deverá criar o `AWSResilienceHubAsssessmentExecutionPolicy`

     usar o procedimento apropriado em the section called “Como o AWS Resilience Hub funciona com IAM”.

2. Para ser notificado quando AWS Resilience Hub detectar qualquer desvio nas políticas de resiliência ou quando seus recursos tiverem sido desviados, ative Receber notificação quando o aplicativo mudar.

   Se essa opção estiver ativada, para receber notificações de deriva, você deverá especificar um tópico do Amazon Simple Notification Service (AmazonSNS). Para fornecer um SNS tópico da Amazon, na seção Fornecer um SNS tópico, selecione Escolher uma opção de SNS tópico e selecione um SNS tópico da Amazon na lista suspensa Escolha um SNS tópico.

   > **Note**
   >
   > - Para permitir AWS Resilience Hub a publicação de notificações em seus SNS tópicos da Amazon, seu SNS tópico da Amazon deve ser configurado com as permissões apropriadas. Para obter mais informações sobre a configuração de permissões, consulte the section called “Habilitando AWS Resilience Hub a publicação em seus SNS tópicos da Amazon”.
   > - As avaliações diárias podem ter um impacto na sua cota para execuções. Para obter mais informações sobre cotas, consulte Endpoints e cotas do AWS Resilience Hub, na Referência geral da AWS .

   Para usar SNS tópicos da Amazon que estão em uma região diferente Conta da AWS ou diferente, ou ambas, selecione Inserir SNS tópico ARN e insira o Nome do recurso da

Amazon (ARN) do SNS tópico da Amazon na caixa Fornecer um SNS tópico. Para obter mais informações sobreARNs, consulte Amazon Resource Names (ARNs) na Referência AWS geral.

Próximo

Etapa 6: configurar permissões

Etapa 6: configurar permissões

AWS Resilience Hub permite que você configure as permissões necessárias para que a conta primária e a conta secundária descubram e avaliem os recursos. No entanto, você deve executar o procedimento separadamente para configurar as permissões para cada conta.

Para configurar IAM funções e IAM permissões

1. Para selecionar uma IAM função existente que será usada para acessar recursos na conta atual, selecione uma IAM função na lista suspensa Selecionar uma IAM função.

   > **Note**
   >
   > Para uma configuração de várias contas, se você não especificar os nomes de recursos da Amazon (ARNs) da IAM função na ARN caixa Insira uma IAM função, AWS Resilience Hub usará a IAM função que você selecionou na lista suspensa Selecionar uma IAM função para todas as contas.

   Se não houver nenhuma IAM função existente vinculada à sua conta, você poderá criar uma IAM função usando uma das seguintes opções:

   - AWS IAMconsole — Se você escolher essa opção, deverá concluir o procedimento em Para criar sua função do hub de AWS resiliência no IAM console.
   - AWS CLI— Se você escolher essa opção, deverá concluir todas as etapas em AWS CLI.
   - CloudFormation modelo — Se você escolher essa opção, dependendo do tipo de conta (conta primária ou conta secundária), deverá criar as funções usando o AWS CloudFormation modelo apropriado.
2. Escolha a seta para a direita para expandir Adicionar IAM função (s) de uma conta cruzada - seção Opcional.

3. Para selecionar IAM funções de uma conta cruzada, insira ARNs a IAM função na ARN caixa Inserir uma IAM função. Certifique-se ARNs de que as IAM funções que você está inserindo não pertençam à conta corrente.
4. Se você quiser usar o IAM usuário atual para descobrir os recursos do seu aplicativo, escolha a seta para a direita para expandir a seção Usar as permissões IAM do usuário atual e selecione Entendo que devo configurar manualmente as permissões para ativar a funcionalidade necessária AWS Resilience Hub.

   Se você selecionar essa opção, alguns dos AWS Resilience Hub recursos (como notificação de desvio) podem não funcionar conforme o esperado e as entradas fornecidas nas etapas 1 e 3 serão ignoradas.

Próximo

Etapa 7: configurar os parâmetros de configuração do aplicativo

Etapa 7: configurar os parâmetros de configuração do aplicativo

Esta seção permite que você forneça os detalhes do seu suporte de failover entre regiões usando. AWS Elastic Disaster Recovery AWS Resilience Hub usará essas informações para fornecer recomendações de resiliência.

Para obter mais informações sobre parâmetros de configuração do aplicativo, consulte Parâmetros de configuração do aplicativo.

Para adicionar parâmetros de configuração do aplicativo (opcional)

1. Para expandir a seção Parâmetros de configuração do aplicativo, escolha a seta direita.
2. Insira o ID da conta de failover na caixa ID da conta. Por padrão, pré-preenchemos esse campo com o ID da sua conta que é usado para AWS Resilience Hub, que pode ser alterado.
3. Selecione uma região de failover na lista suspensa Região.

> **Note**
>
> Se quiser desativar esse recurso, selecione "—" na lista suspensa.

Próximo

Etapa 8: adicionar tags

Etapa 8: adicionar tags

Atribua uma tag ou rótulo a um AWS recurso para pesquisar e filtrar seus recursos ou monitorar seus AWS custos.

(Opcional) Para adicionar tags ao seu aplicativo, escolha Adicionar nova tag se quiser associar uma ou mais tags ao aplicativo. Para obter mais informações sobre etiquetas, consulte Marcação de recursos na Referência geral da AWS .

Escolha Adicionar aplicativo para criar seu aplicativo.

Próximo

Etapa 9: revisar e publicar seu aplicativo do AWS Resilience Hub

Etapa 9: revisar e publicar seu aplicativo do AWS Resilience Hub

Após a publicação, ainda é possível analisar o aplicativo e editar seus recursos. Depois de terminar, escolha Publicar para publicar o aplicativo.

Para obter mais informações sobre a revisão do aplicativo e a edição de seus recursos, consulte o seguinte:

- the section called “Visualizar resumo do aplicativo”
- the section called “Editar recursos de aplicativo”

Próximo

Etapa 10: executar uma avaliação do seu aplicativo do AWS Resilience Hub

Etapa 10: executar uma avaliação do seu aplicativo do AWS Resilience Hub

O aplicativo que você publicou está listado na página Resumo.

Depois de publicar seu AWS Resilience Hub aplicativo, você será redirecionado para a página de resumo do aplicativo, onde poderá executar uma avaliação de resiliência. A avaliação avalia a configuração do seu aplicativo em relação à política de resiliência anexada ao seu aplicativo. É gerado um relatório de avaliação que mostra como seu aplicativo se compara aos objetivos de sua política de resiliência.

Para executar uma avaliação de resiliência

1. Na página Resumo dos aplicativos, escolha Avaliar resiliência.
2. Na caixa de diálogo Executar avaliação de resiliência, insira um nome exclusivo para o relatório ou use o nome gerado na caixa Nome do relatório.
3. Escolha Executar.
4. Depois de ser notificado que o relatório de avaliação foi gerado, escolha a guia Avaliações e sua avaliação para visualizar o relatório.
5. Escolha a guia Revisar para ver o relatório de avaliação de seu aplicativo.

Usando AWS Resilience Hub

AWS Resilience Hub ajuda você a melhorar a resiliência de seus aplicativos AWS e reduzir o tempo de recuperação em caso de paralisação dos aplicativos.

Tópicos:

AWS Resilience Hub painel

O painel fornece uma visão abrangente do status de resiliência do seu portfólio de aplicativos. O painel agrega e organiza eventos de resiliência (por exemplo, banco de dados indisponível ou falha na validação de resiliência), alertas e insights de serviços como o CloudWatch Amazon Fault Injection Service ().AWS FIS

O painel também gera uma pontuação de resiliência para cada aplicativo avaliado. Essa pontuação indica o desempenho do seu aplicativo quando avaliado em relação às políticas de resiliência, alarmes, procedimentos operacionais padrão de recuperação (SOPs) e testes recomendados. Você pode usar essa pontuação para medir as melhorias de resiliência ao longo do tempo.

Para visualizar o AWS Resilience Hub painel, escolha Painel no menu de navegação. A página Painel exibe as seguintes seções:

Status do aplicativo

Os status dos aplicativos indicam se os aplicativos foram avaliados quanto à conformidade com a política de resiliência anexada ou não. Além disso, após a conclusão de uma avaliação, o status

também indica se as fontes de entrada de seus aplicativos foram modificadas ou não. Escolha um número em cada um dos seguintes status para ver todos os aplicativos que compartilham o mesmo status na página Aplicativos:

- Aplicativos na política — Indica todos os aplicativos que estão em conformidade com a política de resiliência anexada.
- Política de violação de aplicativos — Indica todos os aplicativos que não estão em conformidade com a política de resiliência anexada.
- Aplicativos não avaliados — Indica todos os aplicativos cuja conformidade ainda não foi avaliada ou rastreada.
- Aplicativos desviados — Indica todos os aplicativos que se afastaram de sua política de resiliência ou se seus recursos foram desviados.

Pontuação de resiliência de aplicativos ao longo do tempo

Com a pontuação de resiliência do aplicativo ao longo do tempo, você pode visualizar um gráfico da resiliência do seu aplicativo nos últimos 30 dias. Embora o menu suspenso possa listar 10 de seus aplicativos, mostra AWS Resilience Hub apenas um gráfico de até quatro aplicativos por vez. Para obter mais informações sobre a pontuação de resiliência, consulteEntender as pontuações de resiliência.

> **Note**
>
> AWS Resilience Hub não executa avaliações programadas ao mesmo tempo. Como resultado, talvez seja necessário retornar futuramente ao gráfico de pontuação de resiliência ao longo do tempo para visualizar a avaliação diária de seus aplicativos.

AWS Resilience Hub também usa CloudWatch a Amazon para gerar esses gráficos. Escolha Exibir métricas em CloudWatch para criar e visualizar informações mais granulares sobre a resiliência do seu aplicativo em seu CloudWatch painel. Para obter mais informações sobre CloudWatch, consulte Como usar painéis no Guia do CloudWatch usuário da Amazon.

Alarmes implementados

Esta seção lista todos os alarmes que você configurou na Amazon CloudWatch para monitorar todos os aplicativos. Para obter mais informações, consulte Visualizar alarmes.

Experimentos implementados

Esta seção lista todos os experimentos de injeção de falhas que você implementou em todos os aplicativos. Para ter mais informações, consulte Visualizar experimentos de injeção de falhas.

Descrevendo e gerenciando AWS Resilience Hub aplicativos

Um AWS Resilience Hub aplicativo é uma coleção de AWS recursos estruturados para evitar e recuperar interrupções nos AWS aplicativos.

Para descrever um AWS Resilience Hub aplicativo, você fornece um nome do aplicativo, recursos de uma ou mais AWS CloudFormation pilhas e uma política de resiliência apropriada. Você também pode usar qualquer aplicativo do AWS Resilience Hub existente como modelo para descrever seu aplicativo.

Depois de descrever um AWS Resilience Hub aplicativo, você deve publicá-lo para poder executar uma avaliação de resiliência nele. Em seguida, você pode usar as recomendações da avaliação para melhorar a resiliência executando outra avaliação, comparando os resultados e, em seguida, reiterando o processo até que sua carga de trabalho estimada RTO e a carga de trabalho estimada RPO atinjam suas metas. RTO RPO

Para visualizar a página Aplicativos, escolha Aplicativos no painel de navegação. Você pode identificar seus aplicativos na página Aplicativos da seguinte forma:

- Nome: o nome do aplicativo que você forneceu ao defini-lo no AWS Resilience Hub.
- Descrição: a descrição do aplicativo que você forneceu ao defini-lo no AWS Resilience Hub.
- Status de conformidade — AWS Resilience Hub define o status do aplicativo como Avaliado, Não avaliado, Política violada ou Alterações detectadas.
  - AWS Resilience Hub Avaliado - avaliou sua inscrição.
  - Não AWS Resilience Hub avaliado - não avaliou sua inscrição.
  - Política violada - determinou AWS Resilience Hub que seu aplicativo não atendeu aos objetivos de sua política de resiliência para Objetivo de Tempo de Recuperação (RTO) e Objetivo de Ponto de Recuperação (RPO). Analise e use as recomendações fornecidas por AWS Resilience Hub antes de reavaliar sua aplicação quanto à resiliência. Para obter mais informações e recomendações, consulte Adicionar um aplicativo ao AWS Resilience Hub.

  - Alterações detectadas - AWS Resilience Hub detectou alterações feitas na política de resiliência associada ao seu aplicativo. Você deve reavaliar seu aplicativo AWS Resilience Hub para determinar se ele atende aos objetivos da sua política de resiliência.
- Avaliações programadas: o tipo de recurso identifica o recurso do componente para seu aplicativo. Para obter mais informações sobre as avaliações programadas, consulte Resiliência do aplicativo.
  - Ativo: indica que seu aplicativo é avaliado automática e diariamente pelo AWS Resilience Hub.
  - Desativado - Isso indica que sua inscrição não é avaliada automaticamente diariamente AWS Resilience Hub e você deve avaliá-la manualmente.
- Status de desvio — Indica se sua inscrição se desviou ou não da avaliação anterior bem-sucedida e define um dos seguintes status:
  - Com desvio: indica que o aplicativo, que estava em conformidade com sua política de resiliência na avaliação bem-sucedida anterior, agora violou a política de resiliência e está em risco. Além disso, também indica se os recursos nas fontes de entrada, que estão incluídos na versão atual do aplicativo, foram adicionados ou removidos.
  - Não desviado - Indica que a estimativa é de que o aplicativo ainda cumpra suas RPO metas RTO e metas definidas na política. Além disso, também indica que os recursos nas fontes de entrada, que estão incluídos na versão atual do aplicativo, não foram adicionados ou removidos.
- Carga de trabalho estimada RTO — Indica a carga de trabalho máxima estimada possível RTO do seu aplicativo. Esse valor é a carga de trabalho máxima estimada RTO de todos os tipos de interrupção da última avaliação bem-sucedida.
- Carga de trabalho estimada RPO — Indica a carga de trabalho máxima estimada possível RPO do seu aplicativo. Esse valor é a carga de trabalho máxima estimada RTO de todos os tipos de interrupção da última avaliação bem-sucedida.
- Hora da última avaliação: indica a data e a hora em que seu aplicativo foi avaliado pela última vez com sucesso.
- Hora de criação: a data e a hora em que você criou o aplicativo.
- ARN— O nome do recurso Amazon (ARN) do seu aplicativo. Para obter mais informações sobreARNs, consulte Amazon Resource Names (ARNs) na Referência AWS geral.

> **Note**
>
> AWS Resilience Hub pode avaliar totalmente a resiliência dos ECS recursos entre regiões da Amazon somente se você estiver usando a Amazon ECR para o repositório de imagens.

Além disso, você também pode filtrar a lista de aplicativos usando uma das seguintes opções na página Aplicativos:

- Encontrar aplicativos: insira o nome do seu aplicativo para filtrar os resultados pelo nome do seu aplicativo.
- Filtrar o horário da última avaliação por um intervalo de data e hora: para aplicar esse filtro, escolha o ícone do calendário e selecione uma das seguintes opções para filtrar pelos resultados que correspondam ao intervalo de tempo:
  - Intervalo relativo: selecione uma das opções disponíveis e escolha Aplicar.

    Se você escolher a opção Intervalo personalizado, insira uma duração na caixa Inserir duração e selecione a unidade de tempo apropriada na lista suspensa Unidade de tempo e escolha Aplicar.
  - Intervalo absoluto: para especificar o intervalo de data e hora, forneça a hora de início e a hora de término e escolha Aplicar.

Os tópicos a seguir mostram as diferentes abordagens para descrever um AWS Resilience Hub aplicativo e como gerenciá-lo.

Tópicos

Visualizando um resumo AWS Resilience Hub do aplicativo

A página de resumo do aplicativo no AWS Resilience Hub console fornece uma visão geral das informações do aplicativo e da integridade da resiliência.

Visualizar um resumo do aplicativo

1. Escolha Aplicativos no painel de navegação.
2. Na página Aplicativos, escolha o nome do aplicativo que você deseja visualizar.

A página de resumo do aplicativo tem as seguintes seções.

Tópicos

Resumo da avaliação

Esta seção fornece um resumo da última avaliação bem-sucedida e destaca as recomendações críticas como insights acionáveis. AWS Resilience Hub usa os recursos de IA generativa do Amazon Bedrock para ajudar a concentrar os usuários nas recomendações de resiliência mais críticas fornecidas pela. AWS Resilience Hub Ao se concentrar nos itens essenciais, você pode se concentrar nas recomendações mais importantes que melhoram a postura de resiliência do seu aplicativo. Escolha uma recomendação para ver seu resumo e escolha Exibir detalhes para ver mais detalhes sobre as recomendações na seção relevante do relatório de avaliação. Para obter mais informações sobre a revisão do relatório de avaliação, consultethe section called “Analisar relatórios de avaliações”.

> **Note**
>
> - Este resumo da avaliação está disponível somente na região Leste dos EUA (Norte da Virgínia).
> - O resumo da avaliação gerado por grandes modelos de linguagem (LLMs) no Amazon Bedrock são apenas sugestões. O nível atual da tecnologia generativa de IA não é perfeito e não é LLMs infalível. Respostas tendenciosas e incorretas, embora raras, devem ser esperadas. Revise cada recomendação no resumo da avaliação antes de usar a saída de umLLM.

Resumo

Esta seção fornece um resumo do aplicativo selecionado nas seguintes seções:

- Informações do aplicativo — Esta seção fornece as seguintes informações sobre o aplicativo selecionado:
  - Status do aplicativo — Indica o status do aplicativo.
  - Descrição — A descrição do aplicativo.
  - Versão — Indica a versão atualmente avaliada do aplicativo.
  - Política de resiliência — Indica a política de resiliência anexada ao aplicativo. Para obter mais informações sobre políticas de resiliência, consulte Gerenciar políticas de resiliência.
- Desvios de aplicativos — Esta seção destaca os desvios detectados durante a execução de uma avaliação do aplicativo selecionado para verificar se ele está em conformidade com sua política de resiliência. Além disso, ele também verifica se algum dos recursos foi adicionado ou removido desde a última vez em que a versão do aplicativo foi publicada. Esta seção exibe as seguintes informações:
  - Alterações de política — Escolha o número abaixo para ver todos os componentes do aplicativo que estavam em conformidade com a política na avaliação anterior, mas não cumpriram na avaliação atual.
  - Desvios de recursos — Escolha o número abaixo para ver todos os recursos desviados na avaliação mais recente.

Resiliência do aplicativo

As métricas mostradas na seção Pontuação de resiliência são da avaliação de resiliência mais recente do aplicativo.

Pontuações de resiliência

A pontuação de resiliência ajuda você a quantificar seu preparo para lidar com uma possível interrupção. Essa pontuação reflete o quanto seu aplicativo seguiu de perto as AWS Resilience Hub recomendações para atender à política de resiliência, aos alarmes, aos procedimentos operacionais padrão (SOPs) e aos testes do aplicativo.

A pontuação máxima de resiliência que seu aplicativo pode alcançar é 100%. A pontuação representa todos os testes recomendados que são executados em um período de tempo predefinido. Isso indica que os testes estão iniciando o alarme correto e que o alarme inicia o correto. SOP

Por exemplo, suponha que ela AWS Resilience Hub recomende um teste com um alarme e outroSOP. Quando o teste é executado, o alarme inicia o associado eSOP, em seguida, é executado com êxito. Para obter mais informações sobre a pontuação de resiliência, consulte Entender as pontuações de resiliência.

Alarmes implementados

A seção Alarmes implementados do resumo do aplicativo lista os alarmes que você configurou na Amazon CloudWatch para monitorar o aplicativo. Para obter mais informações sobre alarmes, consulte Gerenciar alarmes.

Experimentos implementados

A seção de resumo do aplicativo Experimentos de injeção de falhas mostra uma lista dos experimentos de injeção de falhas. Para obter mais informações sobre os experimentos de injeção de falha, consulte Gerenciando experimentos do Amazon Fault Injection Service.

Editando recursos AWS Resilience Hub do aplicativo

Para receber avaliações de resiliência precisas e úteis, certifique-se de que a descrição do aplicativo esteja atualizada e corresponda ao AWS aplicativo e aos recursos reais. Os relatórios de avaliação, validação e recomendações são baseados nos recursos listados. Se você adicionar ou remover recursos de um AWS aplicativo, deverá refletir essas alterações em AWS Resilience Hub.

AWS Resilience Hub fornece transparência sobre as fontes do seu aplicativo. Você pode identificar e editar os recursos e as fontes do aplicativo em seu aplicativo.

> **Note**
>
> A edição dos recursos modifica somente a AWS Resilience Hub referência do seu aplicativo. Nenhuma alteração é feita em seus recursos reais.

Você pode adicionar recursos que estão faltando, modificar recursos existentes ou remover recursos desnecessários. Os recursos são agrupados em componentes lógicos do aplicativo (AppComponents). Você pode editar o AppComponents para refletir melhor a estrutura do seu aplicativo.

Adicione ou atualize os recursos do seu aplicativo editando uma versão de rascunho do seu aplicativo e publicando as alterações em uma nova versão (de lançamento). AWS Resilience Hub

usa a versão de lançamento (que inclui os recursos atualizados) do seu aplicativo para executar avaliações de resiliência.

Avaliar a resiliência do seu aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o nome do aplicativo que deseja editar.
3. No menu Ações, escolha Avaliar resiliência.
4. Na caixa de diálogo Executar avaliação de resiliência, insira um nome exclusivo para o relatório ou use o nome gerado na caixa Nome do relatório.
5. Escolha Executar.
6. Depois de ser notificado que o relatório de avaliação foi gerado, escolha a guia Avaliações e sua avaliação para visualizar o relatório.
7. Escolha a guia Revisar para ver o relatório de avaliação de seu aplicativo.

Para habilitar a avaliação agendada

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o aplicativo para o qual você deseja habilitar a avaliação agendada.
3. Ative a opção Avaliar automaticamente diariamente.

Para desativar a avaliação agendada

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o aplicativo para o qual você deseja habilitar a avaliação agendada.
3. Desative a opção Avaliar automaticamente diariamente.

> **Note**
>
> Desativar a avaliação agendada desativará a notificação de desvio.

4. Escolha Desativar.

Para habilitar a notificação de desvio para seu aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o aplicativo para o qual você deseja ativar a notificação de desvio ou edite as configurações de notificação de desvio.
3. Você pode editar a notificação de desvio escolhendo uma das seguintes opções:
   - Em Ações, escolha Ativar notificação de desvio.
   - Escolha Ativar notificação na seção Desvios de aplicativos.
4. Conclua as etapas eEtapa 5: configurar avaliações agendadas e notificação de deriva, em seguida, retorne a esse procedimento.
5. Escolha Habilitar.

   Ativar a notificação de desvio também permitirá a avaliação programada.

Para editar a notificação de desvio para seu aplicativo

> **Note**
>
> Esse procedimento é aplicável se você tiver ativado a avaliação programada (a avaliação diária automática está ativada) e a notificação de desvio.

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o aplicativo para o qual você deseja ativar a notificação de desvio ou edite as configurações de notificação de desvio.
3. Você pode editar a notificação de desvio escolhendo uma das seguintes opções:
   - Em Ações, escolha Editar notificação de desvio.
   - Escolha Editar notificação na seção Desvios de aplicativos.
4. Conclua as etapas eEtapa 5: configurar avaliações agendadas e notificação de deriva, em seguida, retorne a esse procedimento.
5. Escolha Salvar.

Para atualizar as permissões de segurança do seu aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o aplicativo para o qual você deseja atualizar as permissões de segurança.
3. Em Ações, escolha Permissões para atualizar.
4. Para atualizar as permissões de segurança, realize as etapas em Etapa 6: configurar permissões e retorne a esse procedimento.
5. Escolha Salvar e atualizar.

Anexar uma política de resiliência ao seu aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o nome do aplicativo que deseja editar.
3. No menu Ações, escolha Anexar política de resiliência.
4. Na caixa de diálogo Anexar política, selecione uma política de resiliência na lista suspensa Selecionar uma política de resiliência.
5. Escolha Anexar.

Para editar fontes de entrada, recursos e AppComponents do seu aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o nome do aplicativo que deseja editar.
3. Escolha a guia Estrutura do aplicativo.
4. Escolha o sinal de adição + antes de Versão e, em seguida, selecione a versão do aplicativo com o status Rascunho.
5. Para editar fontes de entrada, recursos e AppComponents do seu aplicativo, conclua as etapas nos procedimentos a seguir.

Para editar as fontes de entrada do seu aplicativo

1. Para editar as fontes de entrada do seu aplicativo, escolha a guia Fontes de entrada.

   A seção Fontes de entrada lista todas as fontes de entrada dos recursos do seu aplicativo. Você pode identificar as fontes de entrada da seguinte forma:

- Nome da fonte: o nome da fonte de entrada. Escolha o nome de uma fonte para visualizar seus detalhes no respectivo aplicativo. Para fontes de entrada adicionadas manualmente, o link não estará disponível. Por exemplo, se você escolher o nome da fonte importada de uma AWS CloudFormation pilha, você será redirecionado para a página de detalhes da pilha no console. AWS CloudFormation
- ARN da fonte: o nome do recurso da Amazon (ARN) da fonte de entrada. Escolha um ARN para visualizar seus detalhes no respectivo aplicativo. Para fontes de entrada adicionadas manualmente, o link não estará disponível. Por exemplo, se você escolher um ARN importado de uma pilha do AWS CloudFormation , você será redirecionado para a página de detalhes da pilha no console do AWS CloudFormation .
- Tipo de fonte: o tipo da fonte de entrada. As fontes de entrada incluem clusters, AWS CloudFormation pilhas, AppRegistry aplicativos AWS Resource Groups, arquivos de estado do Terraform e recursos adicionados manualmente do Amazon EKS.
- Recursos associados: o número de recursos associados à fonte de entrada. Escolha um número para ver todos os recursos associados de uma fonte de entrada na guia Recursos.

2. Para adicionar fontes de entrada ao seu aplicativo, na seção Fontes de entrada, escolha Adicionar fontes de entrada. Para obter mais informações sobre como adicionar fontes de entrada, consulte the section called “Etapa 3: Adicionar recursos a seu aplicativo AWS Resilience Hub ”.
3. Para editar fontes de entrada, selecione as fontes de entrada e escolha uma das seguintes opções em Ações:

   - Reimportar fontes de entrada (até 5): reimporta até cinco fontes de entrada selecionadas.
   - Excluir fontes de entrada: exclui as fontes de entrada selecionadas.

     Para publicar um aplicativo, ele deve conter no mínimo uma fonte de entrada. Se você excluir todas as fontes de entrada, a opção Publicar nova versão será desativada.

Para editar os recursos do seu aplicativo

1. Para editar os recursos do seu aplicativo, escolha a guia Recursos.

> **Note**
>
> Para ver a lista de recursos não avaliados, escolha Visualizar recursos não avaliados.

A seção Recursos lista os recursos do aplicativo que você escolheu usar como modelo para a descrição do seu aplicativo. Para aprimorar sua experiência de pesquisa, AWS Resilience Hub agrupou recursos com base em vários critérios de pesquisa. Esses critérios de pesquisa incluem AppComponent tipos, recursos não suportados e recursos excluídos. Para filtrar os recursos com base em um critério de pesquisa na tabela Recursos, escolha o número abaixo de cada um dos critérios de pesquisa.

É possível identificar os recursos por:

- ID lógica — Uma ID lógica é um nome usado para identificar recursos em sua AWS CloudFormation pilha, arquivo de estado do Terraform, aplicativo adicionado manualmente, AppRegistry aplicativo ou. AWS Resource Groups

> **Note**
>
> - O Terraform permite que você use o mesmo nome para diferentes tipos de recursos. Portanto, você vê "- tipo de recurso" no final do ID lógico dos recursos que compartilham o mesmo nome.
> - Para visualizar as instâncias de todos os recursos do aplicativo, escolha o sinal de adição (+) antes do ID lógico. Para visualizar todas as instâncias de um recurso do aplicativo, escolha o sinal de adição (+) antes da ID lógica de cada recurso.
>
> Para obter mais informações sobre os recursos com suporte, consulte the section called “ AWS Resilience Hub Recursos suportados”.

- Tipo de recurso: o tipo de recurso identifica o recurso do componente para seu aplicativo. Por exemplo, o `AWS::EC2::Instance` declara uma instância do Amazon EC2. Para obter mais informações sobre o agrupamento de AppComponent recursos, consulteAgrupando recursos em um componente de aplicativo.
- Nome da fonte: o nome da fonte de entrada. Escolha o nome de uma fonte para visualizar seus detalhes no respectivo aplicativo. Para fontes de entrada adicionadas manualmente, o link não estará disponível. Por exemplo, se você escolher o nome da fonte que é importado de uma AWS CloudFormation pilha, você será redirecionado para a página de detalhes da pilha no. AWS CloudFormation

- Tipo de fonte: o tipo da fonte de entrada. As fontes de entrada incluem AWS CloudFormation pilhas, AppRegistry aplicativos AWS Resource Groups, arquivos de estado do Terraform e recursos adicionados manualmente.

> **Note**
>
> Para editar seus clusters do Amazon EKS, realize as etapas no procedimento Editar as fontes de entrada de seu aplicativo AWS Resilience Hub .

- Pilha de origem — A AWS CloudFormation pilha que contém o recurso. Essa coluna depende do tipo de estrutura do aplicativo que você selecionou.
- ID físico: o identificador real atribuído a esse recurso, como o ID de uma instância do Amazon EC2 ou o nome de um bucket do S3.
- Incluído: indica se o AWS Resilience Hub inclui esses recursos no aplicativo.
- Avaliável: indica se o AWS Resilience Hub avaliará seu recurso quanto à resiliência.
- AppComponents— O AWS Resilience Hub componente que foi atribuído a esse recurso quando sua estrutura de aplicativo foi descoberta.
- Nome: nome do recurso do aplicativo.
- Conta — A AWS conta que possui o recurso físico.

2. Para encontrar um recurso que não esteja listado, insira o ID lógico do recurso na caixa de pesquisa.
3. Para remover um recurso do seu aplicativo, selecione o recurso e escolha Excluir recurso em Ações.
4. Para resolver os recursos em seu aplicativo, escolha Atualizar recursos.
5. Para modificar seus recursos de aplicativos existentes, realize as seguintes etapas:

   a. Selecione um recurso e escolha Atualizar pilhas em Ações.

   b. Na página Atualizar pilhas, para atualizar seus recursos, realize os procedimentos apropriados em Etapa 3: adicionar recursos ao seu AWS Resilience Hub aplicativo e, em seguida, retorne a esse procedimento.

   c. Escolha Salvar.

6. Para adicionar um recurso ao seu aplicativo, em Ações, escolha Adicionar recurso e conclua as seguintes etapas:

   a. Selecione um tipo de recurso na lista suspensa Tipo de recurso.

b. Selecione um na AppComponent lista AppComponentsuspensa.

c. Insira o ID lógico do recurso na caixa Nome do recurso.

d. Insira o ID do recurso físico, o nome do recurso ou o ARN do recurso na caixa Identificador do recurso.

e. Escolha Adicionar.

7. Para editar o nome do recurso, selecione um recurso, escolha Editar nome do recurso em Ações e realize as seguintes etapas:

   a. Insira o ID lógico do recurso na caixa Nome do recurso.

   b. Escolha Salvar.

8. Para editar o identificador do recurso, selecione um recurso, escolha Editar identificador do recurso em Ações e realize as seguintes etapas:

   a. Insira o ID do recurso físico, o nome do recurso ou o ARN do recurso na caixa Identificador do recurso.

   b. Escolha Salvar.

9. Para alterar o AppComponent, selecione um recurso, escolha Alterar AppComponent em Ações e conclua as seguintes etapas:

   a. Selecione um na AppComponent lista AppComponentsuspensa.

   b. Escolha Adicionar.

10. Para excluir um recurso, selecione um recurso e escolha Excluir recurso em Ações.

11. Para incluir um recurso, selecione um recurso e escolha Incluir recurso em Ações.

Para editar o AppComponents do seu aplicativo

1. Para editar o AppComponents do seu aplicativo, escolha a AppComponentsguia.

> **Note**
>
> Para obter mais informações sobre o agrupamento de AppComponent recursos, consulte Agrupando recursos em um componente de aplicativo.

A AppComponentsseção lista todos os componentes lógicos nos quais os recursos estão agrupados. Você pode identificá-los AppComponents da seguinte forma:

- AppComponent name — O nome do AWS Resilience Hub componente que foi atribuído a esse recurso quando sua estrutura de aplicativo foi descoberta.
- AppComponent tipo — O tipo de AWS Resilience Hub componente.
- Nome da fonte: o nome da fonte de entrada. Escolha o nome de uma fonte para visualizar seus detalhes no respectivo aplicativo. Por exemplo, se você escolher o nome da fonte importada de uma pilha do AWS CloudFormation , você será redirecionado para a página de detalhes da pilha no AWS CloudFormation.
- Contagem de recursos: o número de recursos associados à fonte de entrada. Escolha um número para ver todos os recursos associados de uma fonte de entrada na guia Recursos.

2. Para criar um AppComponent, no menu Ações, escolha Criar novo AppComponent e conclua as seguintes etapas:
   a. Insira um nome para o AppComponent na caixa de AppComponentnome. Para referência, pré-preenchemos esse campo com um nome de amostra.
   b. Selecione o tipo AppComponent de na lista suspensa AppComponentde tipos.
   c. Escolha Salvar.
3. Para editar um AppComponent, selecione um AppComponent e escolha Editar em AppComponent Ações.
4. Para excluir um AppComponent, selecione um AppComponent e escolha Excluir AppComponent das ações.

Depois de fazer alterações na sua lista de recursos, você receberá um alerta indicando que foram feitas alterações na versão de rascunho do seu aplicativo. Para executar uma avaliação de resiliência precisa, você deve publicar uma nova versão do aplicativo. Para obter mais informações sobre como publicar uma nova versão, consulte Publicando uma nova versão do AWS Resilience Hub aplicativo.

Gerenciando componentes do aplicativo

Um componente de aplicativo (AppComponent) é um grupo de AWS recursos relacionados que funcionam e falham como uma única unidade. Por exemplo, se você tiver um

banco de dados primário e um banco de dados de réplica, os dois bancos de dados pertencem ao mesmo AppComponent. AWS Resilience Hub tem regras que determinam quais AWS recursos podem pertencer a qual AppComponent tipo. Por exemplo, a `DBInstance` pode pertencer `AWS::ResilienceHub::DatabaseAppComponent` a ou não`AWS::ResilienceHub::ComputeAppComponent`.

Eles AWS Resilience Hub AppComponents oferecem suporte aos seguintes recursos:

- `AWS::ResilienceHub::ComputeAppComponent`
  - `AWS::ApiGateway::RestApi`
  - `AWS::ApiGatewayV2::Api`
  - `AWS::AutoScaling::AutoScalingGroup`
  - `AWS::EC2::Instance`
  - `AWS::ECS::Service`
  - `AWS::EKS::Deployment`
  - `AWS::EKS::ReplicaSet`
  - `AWS::EKS::Pod`
  - `AWS::Lambda::Function`
  - `AWS::StepFunctions::StateMachine`
- `AWS::ResilienceHub::DatabaseAppComponent`
  - `AWS::DocDB::DBCluster`
  - `AWS::DynamoDB::Table`
  - `AWS::RDS::DBCluster`
  - `AWS::RDS::DBInstance`
- `AWS::ResilienceHub::NetworkingAppComponent`
  - `AWS::EC2::NatGateway`
  - `AWS::ElasticLoadBalancing::LoadBalancer`
  - `AWS::ElasticLoadBalancingV2::LoadBalancer`
  - `AWS::Route53::RecordSet`
- `AWS:ResilienceHub::NotificationAppComponent`
  - `AWS::SNS::Topic`

- `AWS::ResilienceHub::QueueAppComponent`

  - `AWS::SQS::Queue`
- `AWS::ResilienceHub::StorageAppComponent`
  - `AWS::Backup::BackupPlan`
  - `AWS::EC2::Volume`
  - `AWS::EFS::FileSystem`
  - `AWS::FSx::FileSystem`

> **Note**
>
> Atualmente, AWS Resilience Hub oferece suporte somente ao Amazon FSx para Windows File Server.

  - `AWS::S3::Bucket`

Tópicos

- Agrupando recursos em um componente de aplicativo

Agrupando recursos em um componente de aplicativo

Quando o aplicativo é importado AWS Resilience Hub junto com seus recursos, AWS Resilience Hub faz o possível para agrupar os recursos relacionados no mesmo AppComponent, mas nem sempre é 100% preciso. Além disso, AWS Resilience Hub executa as seguintes atividades depois que seu aplicativo e seus recursos são importados com sucesso:

- Examina seus recursos para verificar se eles podem ser reagrupados em novos AppComponents para melhorar a precisão da avaliação.
- Se AWS Resilience Hub identificar recursos que podem ser reagrupados em novos AppComponents, ele exibe o mesmo que as recomendações e permite que você aceite, modifique (adicione ou remova) ou rejeite os mesmos. Em AWS Resilience Hub, o nível de confiança atribuído a uma recomendação de agrupamento indica o grau de certeza com o qual os recursos devem ser agrupados com base em seus atributos e metadados. Um alto nível de confiança indica AWS Resilience Hub que, com um nível de confiança de 90% ou mais, os recursos desse grupo estão relacionados e devem ser agrupados. Um nível de confiança médio indica que AWS Resilience Hub tem um nível de confiança entre 70% e 90% de que os recursos desse grupo estão relacionados e devem ser agrupados.

> **Note**
>
> AWS Resilience Hub requer o agrupamento correto para que possa calcular a carga de trabalho estimada e a carga de trabalho RTO RPO estimada para gerar recomendações.

Veja a seguir exemplos de agrupamentos corretos:

- Agrupe bancos de dados e réplicas primários em um único AppComponent.
- Agrupe um bucket do Amazon S3 e sua replicação de destino em um único. AppComponent
- Agrupe EC2 instâncias da Amazon que executam o mesmo aplicativo em uma única AppComponent.
- Agrupe uma SQS fila da Amazon e sua fila de mensagens sem saída em uma única. AppComponent
- Agrupe ECS os serviços da Amazon em uma região e faça o failover ECS dos serviços da Amazon em outra região em uma única AppComponent região.

Para obter mais informações sobre como revisar e incluir recomendações de agrupamento de recursos por AWS Resilience Hub, consulte os tópicos a seguir:

- AWS Resilience Hub recomendações de agrupamento de recursos
- Agrupando manualmente os recursos em um AppComponent

AWS Resilience Hub recomendações de agrupamento de recursos

Esta seção explica como gerar e revisar recomendações de agrupamento de recursos em AWS Resilience Hub.

> **Note**
>
> Você pode conceder as IAM permissões necessárias para trabalhar AWS Resilience Hub usando a política `AWSResilienceHubAsssessmentExecutionPolicy` AWS gerenciada. Para obter mais informações sobre a política AWS gerenciada, consulteAWSResilienceHubAsssessmentExecutionPolicy.

Para ver as recomendações de agrupamento de recursos

1. No painel de navegação, escolha Aplicativos.
2. Escolha Adicionar página do aplicativo, escolha o nome do aplicativo para o qual você deseja revisar as recomendações de agrupamento de recursos.
3. Escolha a guia Estrutura do aplicativo.
4. Se AWS Resilience Hub exibir um alerta de informações, escolha Revisar recomendações para ver todas as recomendações de agrupamento de recursos. Caso contrário, conclua as etapas a seguir para gerar manualmente recomendações de agrupamento de recursos:

   a. Escolha atributos.

   b. Escolha Obter recomendações de agrupamento no menu Ações.

      AWS Resilience Hub examina seus recursos para verificar como eles podem ser agrupados da melhor maneira possível em relevantes AppComponents para melhorar a precisão das avaliações. Se AWS Resilience Hub descobrir que seus recursos podem ser agrupados, ele exibirá um alerta de informações sobre os mesmos.

   c. Se o alerta de informações for exibido, escolha Revisar recomendações para ver todas as recomendações de agrupamento de recursos.

   Você pode identificá-los AppComponents na seção Revisar recomendações de agrupamento de recursos usando o seguinte:

   - AppComponent name — Nome do AppComponent em que os recursos serão agrupados.
   - Nível de confiança — Indica o nível de confiança do AWS Resilience Hub na recomendação de agrupamento.
   - Contagem de recursos — Indica o número de recursos que serão agrupados no AppComponent.
   - AppComponent tipo — Indica o tipo de AppComponent.

Para visualizar os recursos que serão agrupados em AppComponents

1. Conclua as etapas do Para ver as recomendações de agrupamento de recursosprocedimento e, em seguida, retorne a esse procedimento.
2. Na seção Revisar recomendações de agrupamento de recursos, marque a caixa de seleção (ao lado do AppComponent nome) para visualizar todos os recursos que serão agrupados dentro

dos selecionados. AppComponent Se você marcar várias caixas de seleção, AWS Resilience Hub exibirá uma seção selecionada de recomendações gerada dinamicamente que agrupa as selecionadas AppComponents em seus respectivos AppComponent tipos. Escolha o número abaixo AppComponent de cada tipo para ver todos os recursos que serão agrupados dentro do selecionado AppComponent.

Você pode identificar os recursos que serão agrupados nos selecionados AppComponent na seção Recursos usando o seguinte:

- ID lógica — Indica a ID lógica do recurso. Um ID lógico é um nome usado para identificar recursos em sua AWS CloudFormation pilha, arquivo de estado do Terraform, aplicativo adicionado manualmente, AppRegistry aplicativo ou. AWS Resource Groups
- ID física — O identificador real atribuído ao recurso, como um ID de EC2 instância da Amazon ou um nome de bucket do Amazon S3.
- Tipo — Indica o tipo de recurso.
- Região — AWS Região na qual o recurso está localizado.

Para aceitar recomendações de agrupamento de recursos

1. Conclua as etapas do Para ver as recomendações de agrupamento de recursosprocedimento e, em seguida, retorne a esse procedimento.
2. Na seção Revisar recomendações de agrupamento de recursos, marque todas as caixas de seleção adjacentes ao AppComponentnome. Para encontrar um específico AppComponent, insira o AppComponent nome na AppComponents caixa Localizar.

   > **Note**
   >
   > Por padrão, AWS Resilience Hub exibe todas as recomendações de agrupamento de recursos. Para filtrar a tabela com recomendações de agrupamento de recursos rejeitadas anteriormente, escolha Rejeitado anteriormente no menu suspenso ao lado da caixa Localizar. AppComponents

3. Escolha Accept (Aceitar).
4. Escolha Aceitar na caixa de diálogo Aceitar recomendação de agrupamento de recursos.

   AWS Resilience Hub exibirá um alerta informativo se o agrupamento de recursos for bem-sucedido. Se você aceitou somente um subconjunto de recomendações de agrupamento

de recursos, a seção Revisar recomendações de agrupamento de recursos exibirá todas as recomendações de agrupamento de recursos que você não aceitou.

Para rejeitar recomendações de agrupamento de recursos

1. Conclua as etapas do Para ver as recomendações de agrupamento de recursosprocedimento e, em seguida, retorne a esse procedimento.
2. Na seção Revisar recomendações de agrupamento de recursos, marque todas as caixas de seleção adjacentes ao AppComponentnome. Para encontrar um específico AppComponent, insira o AppComponent nome na AppComponents caixa Localizar.

   > **Note**
   >
   > Por padrão, AWS Resilience Hub exibe todas as recomendações de agrupamento de recursos. Para filtrar a tabela com recomendações de agrupamento de recursos rejeitadas anteriormente, selecione Rejeitado anteriormente no menu suspenso ao lado da caixa Localizar. AppComponents

3. Escolha Rejeitar.
4. Selecione um dos motivos para rejeitar a recomendação de agrupamento de recursos e escolha Rejeitar na caixa de diálogo Rejeitar recomendação de agrupamento de recursos.

   AWS Resilience Hub exibe um alerta informativo confirmando o mesmo. Se você rejeitou somente um subconjunto de recomendações de agrupamento de recursos, a seção Revisar recomendações de agrupamento de recursos exibirá todas as recomendações de agrupamento de recursos que você não aceitou.

Agrupando manualmente os recursos em um AppComponent

Esta seção explica como agrupar recursos manualmente em um AppComponent e atribuir diferentes AppComponent a um recurso em AWS Resilience Hub.

Para agrupar recursos

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o nome do aplicativo que contém os recursos que você deseja reagrupar.

3. Escolha a guia Estrutura do aplicativo.
4. Na guia Versão, selecione a versão do aplicativo com status Rascunho.
5. Escolha a guia Recursos.
6. Marque as caixas de seleção adjacentes à ID lógica para selecionar todos os recursos que você deseja agrupar.

> **Note**
>
> Você não pode escolher recursos adicionados manualmente.

7. Escolha Ações e selecione Recursos do grupo.
8. Escolha um na AppComponent lista AppComponent suspensa Escolher na qual você deseja agrupar o recurso.
9. Escolha Salvar.
10. Escolha Publicar nova versão.
11. Escolha a guia Estrutura do aplicativo.
12. Para visualizar a versão publicada do seu aplicativo, realize as seguintes etapas:
    a. Na guia Versão, selecione a versão do aplicativo com status Liberação atual.
    b. Escolha a guia Recursos.

Para atribuir recursos a um AppComponent

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o nome do aplicativo que contém o recurso que você deseja reagrupar.
3. Escolha a guia Estrutura do aplicativo.
4. Em Versão, selecione a versão do aplicativo com status Rascunho.
5. Escolha a guia Recursos.
6. Marque a caixa de seleção adjacente à ID lógica para selecionar o recurso.
7. Escolha Alterar no AppComponent menu Ações.
8. Para excluir o atual AppComponent da AppComponentseção, escolha X no canto superior direito do rótulo que exibe seu nome atual AppComponent .

9. Para agrupar o recurso em um diferente AppComponent, escolha um AppComponent diferente na AppComponent lista suspensa Escolher.
10. Escolha Adicionar.
11. Exclua qualquer vazio AppComponents da AppComponentsguia.
12. Escolha Publicar nova versão.
13. Escolha a guia Estrutura do aplicativo.
14. Para visualizar a versão publicada do seu aplicativo, realize as seguintes etapas:

    a. Na guia Versão, selecione a versão do aplicativo com status Liberação atual.

    b. Escolha a guia Recursos.

Publicando uma nova versão do AWS Resilience Hub aplicativo

Depois de fazer alterações nos recursos do AWS Resilience Hub aplicativo, conforme descrito emEditando recursos AWS Resilience Hub do aplicativo, você deve publicar uma nova versão do seu aplicativo para executar uma avaliação precisa da resiliência. Além disso, talvez seja necessário publicar uma nova versão do seu aplicativo se tiver adicionado novos alarmes e testes recomendados ao seu aplicativo. SOPs

Para publicar a nova versão de seu aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, escolha o nome do aplicativo.
3. Escolha a guia Estrutura do aplicativo.
4. Escolha Publicar nova versão.
5. Na caixa de diálogo Publicar versão, na caixa Nome, insira um nome para a versão do aplicativo ou você pode usar o nome padrão sugerido por AWS Resilience Hub.
6. Escolha Publicar.

   Quando você publica uma nova versão do seu aplicativo, ela se torna a versão que é avaliada quando você executa avaliações de resiliência. Além disso, a versão preliminar será idêntica à versão lançada até que você faça alguma alteração.

Depois de publicar uma nova versão do seu aplicativo, recomendamos que você execute um novo relatório de avaliação de resiliência para confirmar que seu aplicativo ainda atende à sua política

de resiliência. Para obter informações sobre como executar uma avaliação, consulte Executando e gerenciando avaliações de AWS Resilience Hub resiliência.

Visualizando todas as versões do AWS Resilience Hub aplicativo

Para ajudar a rastrear as alterações do aplicativo, AWS Resilience Hub exibe as versões anteriores do seu aplicativo a partir do momento em que ele foi criado AWS Resilience Hub.

Para visualizar todas as versões do seu aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, escolha o nome do aplicativo.
3. Escolha a guia Estrutura do aplicativo.
4. Para visualizar todas as versões anteriores do seu aplicativo, escolha o sinal de adição (+) antes de Exibir todas as versões. AWS Resilience Hub indica a versão preliminar e a versão lançada recentemente do seu aplicativo usando os status Rascunho e Versão atual, respectivamente. Você pode escolher qualquer versão do seu aplicativo para visualizar seus recursos AppComponent, fontes de entrada e outras informações associadas.

   Além disso, é possível filtrar a lista usando uma das seguintes opções:

   - Filtrar por nome da versão: insira um nome para filtrar os resultados pelo nome da versão do seu aplicativo.
   - Filtrar por um intervalo de data e hora: para aplicar esse filtro, escolha o ícone do calendário e selecione uma das seguintes opções para filtrar pelos resultados que correspondam ao intervalo de tempo:
     - Intervalo relativo: selecione uma das opções disponíveis e escolha Aplicar.

       Se você escolher a opção Intervalo personalizado, insira uma duração na caixa Inserir duração e selecione a unidade de tempo apropriada na lista suspensa Unidade de tempo e escolha Aplicar.
     - Intervalo relativo: para especificar o intervalo de data e hora, forneça a hora de início e a hora de término e escolha Aplicar.

Visualizando recursos do AWS Resilience Hub aplicativo

Para visualizar os recursos do seu aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o aplicativo para o qual você deseja atualizar as permissões de segurança.
3. Em Ações, escolha Exibir recursos.

   Na guia Recursos, você pode identificar recursos na tabela Recursos da seguinte forma:

   - ID lógica — Uma ID lógica é um nome usado para identificar recursos em sua AWS CloudFormation pilha, arquivo de estado do Terraform, aplicativo adicionado manualmente, AppRegistry aplicativo ou. AWS Resource Groups

     > **Note**
     >
     > - O Terraform permite que você use o mesmo nome para diferentes tipos de recursos. Portanto, você vê "- tipo de recurso" no final do ID lógico dos recursos que compartilham o mesmo nome.
     > - Para visualizar as instâncias de todos os recursos do aplicativo, escolha o sinal de adição (+) antes do ID lógico. Para visualizar todas as instâncias de um recurso do aplicativo, escolha o sinal de adição (+) antes da ID lógica de cada recurso.
     >
     > Para obter mais informações sobre os recursos com suporte, consulte the section called “ AWS Resilience Hub Recursos suportados”.

   - Status: indica se o AWS Resilience Hub avaliará seu recurso quanto à resiliência.
   - Tipo de recurso: o tipo de recurso identifica o recurso do componente para seu aplicativo. Por exemplo, `AWS::EC2::Instance` declara uma EC2 instância da Amazon. Para obter mais informações sobre o agrupamento de AppComponent recursos, consulteAgrupando recursos em um componente de aplicativo.
   - Nome da fonte: o nome da fonte de entrada. Escolha o nome de uma fonte para visualizar seus detalhes no respectivo aplicativo. Para fontes de entrada adicionadas manualmente, o link não estará disponível. Por exemplo, se você escolher o nome da fonte que é importado de uma AWS CloudFormation pilha, você será redirecionado para a página de detalhes da pilha no. AWS CloudFormation

- Tipo de fonte: o tipo da fonte de entrada.
- AppComponent tipo — O tipo de fonte de entrada. As fontes de entrada incluem AWS CloudFormation pilhas, AppRegistry aplicativos AWS Resource Groups, arquivos de estado do Terraform e recursos adicionados manualmente.

> **Note**
>
> Para editar seus EKS clusters da Amazon, conclua as etapas em Para editar as fontes de entrada do seu procedimento de AWS Resilience Hub inscrição.

- ID física — O identificador real atribuído para esse recurso, como um ID de EC2 instância da Amazon ou um nome de bucket do S3.
- Incluído: indica se o AWS Resilience Hub inclui esses recursos no aplicativo.
- AppComponents— O AWS Resilience Hub componente que foi atribuído a esse recurso quando sua estrutura de aplicativo foi descoberta.
- Nome: nome do recurso do aplicativo.
- Conta — A AWS conta que possui o recurso físico.

4. Escolha Salvar e atualizar.

Excluindo um aplicativo AWS Resilience Hub

Depois de atingir o limite máximo de dez aplicativos, você deve excluir um ou mais aplicativos antes de poder adicionar mais.

Como excluir uma aplicação

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o aplicativo que deseja excluir.
3. Escolha Ações e Excluir aplicativo.
4. Para confirmar a exclusão, digite Excluir na caixa Excluir e escolha Excluir.

Parâmetros de configuração do aplicativo

AWS Resilience Hub fornece um mecanismo de entrada para coletar informações adicionais sobre os recursos associados aos seus aplicativos. Com essas informações, AWS Resilience Hub obterá

uma compreensão mais profunda de seus recursos e fornecerá melhores recomendações de resiliência.

A seção Parâmetros de configuração do aplicativo lista todos os parâmetros de configuração do seu suporte de failover entre regiões para o AWS Elastic Disaster Recovery. Você pode identificar os parâmetros de configuração da seguinte forma:

- Tópico: indica a área do seu aplicativo que está configurada. Por exemplo, configuração de failover.
- Propósito — Indica o motivo pelo qual AWS Resilience Hub solicitou as informações.
- Parâmetro — Indica os detalhes específicos da área de aplicação, que AWS Resilience Hub serão usados para fornecer recomendações para sua aplicação. Atualmente, esse parâmetro usa um valor-chave de somente uma região de failover e uma conta associada.

Atualizar parâmetros de configuração do aplicativo

Esta seção permite que você atualize os parâmetros de configuração do seu aplicativo AWS Elastic Disaster Recovery e publique o aplicativo para incluir os parâmetros atualizados para avaliações de resiliência.

Atualizar os parâmetros de configuração do aplicativo

1. No painel de navegação, escolha Aplicativos.
2. Na página Aplicativos, selecione o nome do aplicativo que deseja editar.
3. Escolha a guia Parâmetros de configuração do aplicativo.
4. Escolha Atualizar.
5. Insira o ID da conta de failover na caixa ID da conta.
6. Selecione uma região de failover na lista suspensa Região.

> **Note**
>
> Se quiser desativar esse recurso, selecione "—" na lista suspensa.

7. Escolha Atualizar e publicar.

Gerenciar políticas de resiliência

Esta seção descreve como criar políticas de resiliência para seus aplicativos. Definir políticas de resiliência corretamente permite que você entenda a postura de resiliência do seu aplicativo. Uma política de resiliência contém informações e objetivos que você usa para avaliar se estima-se que seu aplicativo se recupere de um tipo de interrupção, como software, hardware, zona de disponibilidade ou AWS região. Essas políticas não alteram nem afetam um aplicativo real. Vários aplicativos podem ter a mesma política de resiliência.

Ao criar uma política de resiliência, você define os objetivos de meta: objetivo de tempo de recuperação (RTO) e o objetivo de ponto de recuperação (RPO). Os objetivos determinam se o aplicativo atende à política de resiliência. Anexe a política ao seu aplicativo e execute uma avaliação de resiliência. Você pode criar políticas diferentes para os diferentes tipos de aplicativos em seu portfólio. Por exemplo, um aplicativo de negociação em tempo real teria uma política de resiliência diferente de um aplicativo de relatórios mensais.

> **Note**
>
> AWS Resilience Hub permite que você insira um valor zero nos campos RTO e RPO da sua política de resiliência. Mas, ao avaliar seu aplicativo, o menor resultado de avaliação possível é próximo de zero. Portanto, se você inserir um valor zero nos campos RTO e RPO, o resultado do RTO estimado da workload e do RPO estimado da workload será próximo de zero e o status de conformidade do seu aplicativo será definido como Política violada.

A avaliação avalia a configuração do seu aplicativo em relação à política de resiliência anexada. Ao final do processo, AWS Resilience Hub fornece uma avaliação de como seu aplicativo se compara às metas de recuperação em sua política de resiliência.

Você pode criar políticas de resiliência em Aplicativos e também em Políticas de resiliência. Você pode acessar detalhes relevantes sobre suas políticas e também modificá-las e excluí-las.

AWS Resilience Hub usa suas metas de RTO e RPO para medir a resiliência desses tipos potenciais de interrupções:

- Aplicativo: perda de um serviço ou processo de software necessário.
- Infraestrutura de nuvem: perda de hardware, como instâncias do EC2.

- Zona de disponibilidade (AZ) da infraestrutura de nuvem: uma ou mais zonas de disponibilidade não estão disponíveis.
- Região da infraestrutura de nuvem: uma ou mais regiões não estão disponíveis.

AWS Resilience Hub permite que você crie políticas de resiliência personalizadas ou use nossas políticas de resiliência de padrão aberto e recomendadas. Ao criar políticas personalizadas, nomeie e descreva sua política e escolha a camada ou nível apropriado que define sua política. Esses níveis incluem: serviços básicos de TI, de missão crítica, crítico, importante e não crítico.

Escolha o nível apropriado para sua classe de aplicativo. Por exemplo, você pode classificar um sistema de negociação em tempo real como crítico, enquanto pode classificar um aplicativo de relatórios mensais como não crítico. Ao usar nossas políticas padrão, você pode escolher uma política de resiliência com um nível pré-configurado e valores para as metas de RTO e RPO por tipo de interrupção. Se necessário, você pode alterar o nível e as metas de RTO e RPO.

Você pode criar políticas de resiliência em Políticas de resiliência ou ao descrever um novo aplicativo.

Criar políticas de resiliência

Em AWS Resilience Hub, você pode criar uma política de resiliência. Uma política de resiliência contém informações e objetivos que você usa para avaliar se seu aplicativo pode se recuperar de um tipo de interrupção, como software, hardware, zona de disponibilidade ou AWS região. Essas políticas não alteram nem afetam um aplicativo real. Vários aplicativos podem ter a mesma política de resiliência.

Ao criar uma política de resiliência, você define as metas de objetivo de tempo de recuperação (RTO) e o objetivo de ponto de recuperação (RPO). Quando você executa uma avaliação, AWS Resilience Hub determina se estima-se que o aplicativo atenda aos objetivos definidos na política de resiliência.

A avaliação avalia a configuração do seu aplicativo em relação à política de resiliência anexada. Ao final do processo, AWS Resilience Hub fornece uma avaliação de como seu aplicativo se compara aos objetivos de sua política de resiliência.

> **Note**
>
> AWS Resilience Hub permite que você insira um valor zero nos campos RTO e RPO da sua política de resiliência. Mas, ao avaliar seu aplicativo, o menor resultado de avaliação

possível é próximo de zero. Portanto, se você inserir um valor zero nos campos RTO e RPO, o resultado do RTO estimado da workload e do RPO estimado da workload será próximo de zero e o status de conformidade do seu aplicativo será definido como Política violada.

Você pode criar políticas de resiliência em Aplicativos e também em Políticas de resiliência. Você pode acessar detalhes relevantes sobre suas políticas e também modificá-las e excluí-las.

Para criar políticas de resiliência em Aplicativos

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Conclua os procedimentos de the section called “Etapa 1: comece adicionando uma aplicativo” a the section called “Etapa 8: adicionar tags ao seu aplicativo ”.
3. Na seção Políticas de resiliência, escolha Criar política de resiliência.

   A página Criar política de resiliência é exibida.
4. Na seção Escolha um método de criação, selecione Criar uma política.
5. Insira um nome para a política.
6. (Opcional) Insira uma descrição para o perfil.
7. Escolha uma das seguintes opções na lista suspensa Nível:

   - Serviços básicos de TI
   - Missão crítica
   - Crítico
   - Importante
   - Não crítico
8. Para metas de RTO e RPO, em RTO e RPO do aplicativo do cliente, insira um valor numérico na caixa e escolha a unidade de tempo que o valor representa.

   Repita essas entradas em RTO e RPO de infraestrutura para Infraestrutura e Zona de disponibilidade.
9. (Opcional) Se você tiver um aplicativo em várias regiões, talvez queira definir as metas de RTO e RPO de uma região.

   Ative Região. Para as metas de RTO e RPO da Região, em RTO e RPO do aplicativo do cliente, insira um valor numérico na caixa e escolha a unidade de tempo que o valor representa.

10. (Opcional) Se quiser adicionar tags, você pode fazer isso mais tarde, enquanto continua criando sua política. Para obter mais informações sobre etiquetas, consulte Marcação de recursos na Referência geral da AWS .
11. Escolha Criar para criar a política.

Para criar políticas de resiliência em Políticas de resiliência

1. No menu de navegação esquerdo, escolha Políticas.
2. Na seção Políticas de resiliência, escolha Criar política de resiliência.

   A página Criar política de resiliência é exibida.
3. Insira um nome para a política.
4. (Opcional) Insira uma descrição para o perfil.
5. Escolha uma das seguintes opções em Nível:
   - Serviços básicos de TI
   - Missão crítica
   - Crítico
   - Importante
   - Não crítico
6. Para metas de RTO e RPO, em RTO e RPO do aplicativo do cliente, insira um valor numérico na caixa e escolha a unidade de tempo que o valor representa.

   Repita essas entradas em RTO e RPO de infraestrutura para Infraestrutura e Zona de disponibilidade.
7. (Opcional) Se você tiver um aplicativo em várias regiões, talvez queira definir as metas de RTO e RPO de uma região.

   Ative Região. Para metas de RTO e RPO, em RTO e RPO do aplicativo do cliente, insira um valor numérico na caixa e escolha a unidade de tempo que o valor representa.
8. (Opcional) Se quiser adicionar tags, você pode fazer isso mais tarde, enquanto continua criando sua política. Para obter mais informações sobre etiquetas, consulte Marcação de recursos na Referência geral da AWS .
9. Escolha Criar para criar a política.

Para criar políticas de resiliência com base em uma política sugerida

1. No menu de navegação esquerdo, escolha Políticas.
2. Na seção Escolha um método de criação, selecione Selecionar uma política com base em uma política sugerida.
3. Na seção Políticas de resiliência, escolha Criar política de resiliência.

   A página Criar política de resiliência é exibida.
4. Insira um nome para a política de resiliência.
5. (Opcional) Insira uma descrição para o perfil.
6. Na seção Políticas de resiliência sugeridas, visualize e escolha um dos seguintes níveis de política de resiliência predeterminados:

   - Aplicativo não crítico
   - Aplicativo importante
   - Aplicativo crítico
   - Aplicativo crítico global
   - Aplicativo de missão crítica
   - Aplicativo de missão crítica global
   - Serviço básico central
7. Para criar a política de resiliência, escolha Criar política.

Acessar os detalhes da política de resiliência

Ao abrir uma política de resiliência, você vê detalhes importantes sobre a política. Você também pode editar ou excluir a resiliência.

Os detalhes da política de resiliência consistem em duas exibições principais: Resumo e Tags.

Resumo

Informações básicas

Fornece as seguintes informações sobre a política de resiliência: nome, descrição, nível, nível de custo e data de criação.

RTO estimado da workload e RPO estimado da workload

Mostra o RTO estimado da workload e o tipo estimado de interrupção do RPO estimado da workload associado a essa política de resiliência.

Tags

Use essa exibição para gerenciar, adicionar e excluir tags internas deste aplicativo.

Para editar políticas de resiliência em Detalhes da política de resiliência

1. No menu de navegação esquerdo, escolha Políticas.
2. Em Políticas de resiliência, abra uma política de resiliência.
3. Selecione a opção Editar. Insira as alterações apropriadas nos campos Informações básicas e RTO e RPO. Em seguida, escolha Salvar alterações.

Para editar políticas de resiliência na Política de resiliência

1. No menu de navegação esquerdo, escolha Políticas.
2. Em Políticas de resiliência, escolha uma política de resiliência.
3. Escolha Ações e, em seguida, selecione Editar.
4. Insira as alterações apropriadas nos campos Informações básicas e RTO e RPO. Em seguida, escolha Salvar alterações.

Para excluir políticas de resiliência nos Detalhes da política de resiliência

1. No menu de navegação esquerdo, escolha Políticas.
2. Em Políticas de resiliência, abra uma política de resiliência.
3. Escolha Excluir. Confirme a exclusão e escolha Excluir.

Para excluir políticas de resiliência na Política de resiliência

1. No menu de navegação esquerdo, escolha Políticas.
2. Em Políticas de resiliência, escolha uma política de resiliência.
3. Selecione Ações e escolha Excluir.
4. Confirme a exclusão e escolha Excluir.

Executando e gerenciando avaliações de AWS Resilience Hub resiliência

Quando seu aplicativo muda, você deve executar uma avaliação de resiliência. A avaliação compara a configuração de cada componente do aplicativo com a política e faz recomendações de SOP alarmes e testes. Essas recomendações de configuração podem melhorar a velocidade dos procedimentos de recuperação.

As recomendações de alarmes ajudam você a definir alarmes que detectam interrupções. SOPas recomendações fornecem scripts que gerenciam processos comuns de recuperação, como a recuperação de um backup. As recomendações de teste oferecem sugestões para verificar se suas configurações funcionam corretamente. Por exemplo, você pode testar se um aplicativo se recupera durante processos de recuperação automática, como escalabilidade automática ou balanceamento de carga devido a problemas de rede. Você pode testar se os alarmes do aplicativo são acionados quando os recursos atingem seus limites. Você também pode testar o quão bem SOPs funciona nas condições que você indicar.

Executar avaliações de resiliência

Você pode executar um relatório de avaliação de resiliência em vários locais no AWS Resilience Hub. Para obter mais informações sobre seu aplicativo, consulte the section called “Gerenciar aplicações”.

Para executar uma avaliação de resiliência no menu Ações

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Escolha um aplicativo na tabela Aplicativos.
3. Escolha Avaliar resiliência no menu Ações.
4. Na caixa de diálogo Executar avaliação de resiliência, você pode inserir um nome exclusivo ou usar o nome gerado para a avaliação.
5. Escolha Executar.

   Para revisar o relatório de avaliação, escolha Avaliações em seu aplicativo. Para obter mais informações, consulte the section called “Analisar relatórios de avaliações”.

Para executar uma avaliação de resiliência na guia Avaliações

Você pode executar uma nova avaliação de resiliência quando seu aplicativo ou sua política de resiliência mudarem.

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Escolha um aplicativo na tabela Aplicativos.
3. Escolha a guia Avaliações.
4. Escolha Executar avaliação de resiliência.
5. Na caixa de diálogo Executar avaliação de resiliência, você pode inserir um nome exclusivo ou usar o nome gerado para a avaliação.
6. Escolha Executar.

   Para revisar o relatório de avaliação, escolha Avaliações em seu aplicativo. Para obter mais informações, consulte the section called “Analisar relatórios de avaliações”.

Analisar relatórios de avaliações

Você encontra relatórios de avaliação na exibição Avaliações de seu aplicativo.

Para encontrar um relatório de avaliação

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Em Aplicativos, abra um aplicativo.
3. Na guia Avaliações, escolha um relatório de avaliação na tabela Avaliações de resiliência.

Durante a abertura do relatório, você visualiza as seguintes informações:

- Uma visão geral do relatório de avaliação
- Recomendações para melhorar a resiliência.
- Recomendações para configurar alarmes SOPs e testes
- Como criar e gerenciar tags para pesquisar e filtrar seus AWS recursos

Revisar

Esta seção fornece uma visão geral do relatório de avaliação. AWS Resilience Hub lista cada tipo de interrupção e o componente de aplicativo associado. Ele também lista suas RPO políticas reais RTO e determina se o componente do aplicativo pode atingir as metas da política.

Visão geral

Mostra o nome do aplicativo, o nome da política de resiliência e a data de criação do relatório.

Desvios de recursos detectados

Esta seção lista todos os recursos que foram adicionados ou removidos depois de serem incluídos na versão mais recente do aplicativo publicado. Escolha Reimportar fontes de entrada para reimportar todas as fontes de entrada (que contêm recursos desviados) na guia Fontes de entrada. Escolha Publicar e avaliar para incluir os recursos atualizados no aplicativo e receber uma avaliação precisa da resiliência.

Você pode identificar as fontes de entrada desviadas usando o seguinte:

- ID lógica — Indica a ID lógica do recurso. Um ID lógico é um nome usado para identificar recursos em sua AWS CloudFormation pilha, arquivo de estado do Terraform, aplicativo adicionado manualmente, AppRegistry aplicativo ou. AWS Resource Groups
- Alteração — Indica se um recurso de entrada foi adicionado ou removido.
- Nome da fonte — Indica o nome do recurso. Escolha o nome de uma fonte para visualizar seus detalhes no respectivo aplicativo. Para fontes de entrada adicionadas manualmente, o link não estará disponível. Por exemplo, se você escolher o nome da fonte importada de uma AWS CloudFormation pilha, você será redirecionado para a página de detalhes da pilha no. AWS CloudFormation
- Tipo de recurso — Indica o tipo de recurso.
- Conta — Indica a AWS conta que possui o recurso físico.
- Região — Indica a AWS região em que o recurso está localizado.

RTO

Mostra uma representação gráfica que indica se o aplicativo está estimado para atender aos objetivos da política de resiliência. Isso é baseado na quantidade de tempo em que um aplicativo

pode ficar inativo sem causar danos significativos à organização. A avaliação fornece uma carga de trabalho RTO estimada.

RPO

Mostra uma representação gráfica que indica se o aplicativo está estimado para atender aos objetivos da política de resiliência. Isso é baseado na quantidade de tempo em que os dados podem ser perdidos antes que um dano significativo à empresa ocorra. A avaliação fornece uma carga de trabalho RPO estimada.

Detalhes

Fornece descrições detalhadas de cada tipo de interrupção usando as guias Todos os resultados e Desvios de conformidade do aplicativo. A guia Todos os resultados mostra todas as interrupções, incluindo desvios de conformidade, e a guia Desvios de conformidade do aplicativo exibe apenas desvios de conformidade. O tipo de interrupção inclui Aplicativo, infraestrutura de nuvem (Infraestrutura e Zona de disponibilidade) e Região, e fornece as seguintes informações sobre isso:

- AppComponent

  Os recursos que compõem o aplicativo. Por exemplo, seu aplicativo pode ter um componente de banco de dados ou computação.

- Estimado RTO

  Indica se a configuração da política está alinhada com os requisitos da política. Fornecemos dois valores, nosso estimado RTO e seu alvo RTO. Por exemplo, se você ver o valor de 2h em Alvo RTO e 40m em Carga de trabalho estimada RTO, isso indica que fornecemos uma carga de trabalho estimada RTO de 40 minutos, enquanto a atual do seu aplicativo é RTO de duas horas. Baseamos nosso RTO cálculo de carga de trabalho estimada na configuração, não na política. Como resultado, um banco de dados de várias zonas de disponibilidade terá a mesma carga de trabalho estimada RTO para falhas na zona de disponibilidade, independentemente da política selecionada.

- RTOderiva

  Indica a duração pela qual sua inscrição se afastou da carga de trabalho estimada RTO da avaliação anterior bem-sucedida. Fornecemos dois valores, nossa estimativa RTO e RTOderiva. Por exemplo, se você ver o valor de 2h em Estimado RTO e 40m em RTODesvio, isso indica que

seu aplicativo se desvia da carga de trabalho estimada RTO da avaliação anterior bem-sucedida em 40 minutos.

- Estimado RPO

  Mostra a RPO política real de carga de trabalho estimada que é AWS Resilience Hub estimada, com base na RPO política direcionada que você define para cada componente do aplicativo. Por exemplo, você pode ter definido a RPO meta em sua política de resiliência para falhas na Zona de Disponibilidade em uma hora. O resultado estimado pode ser calculado próximo de zero. Isso pressupõe que o Amazon Aurora, onde confirmamos todas as transações, seja bem-sucedido em quatro dos seis nós, abrangendo várias zonas de disponibilidade. Pode levar cinco minutos para a point-in-time restauração.

  A única RTO RPO meta que você pode optar por não fornecer é a Região. Para alguns aplicativos, é útil planejar a recuperação quando há uma dependência crucial de um AWS serviço, que pode ficar indisponível em toda a região.

  Se você escolher essa opção, como definição RTO ou RPO metas para a região, receberá um tempo estimado de recuperação e recomendações operacionais para essas falhas.

- RPOderiva

  Indica a duração pela qual sua inscrição se afastou da carga de trabalho estimada RPO da avaliação anterior bem-sucedida. Fornecemos dois valores, nossa estimativa RPO e RPOderiva. Por exemplo, se você ver o valor de 2h em Estimado RPO e 40m em RPODesvio, isso indica que seu aplicativo se desvia da carga de trabalho estimada RPO da avaliação anterior bem-sucedida em 40 minutos.

Analisar recomendações de resiliência

As recomendações de resiliência avaliam os componentes do aplicativo e recomendam como otimizar a carga de trabalho estimada RTO e a carga de trabalho estimadaRPO, os custos e as mudanças mínimas.

Com AWS Resilience Hub, você pode otimizar a resiliência usando uma das seguintes opções recomendadas em Por que você deve escolher essa opção:

> **Note**
>
> - AWS Resilience Hub fornece até três opções AWS Resilience Hub recomendadas.
> - Se você definir regiões RTO e RPO metas, AWS Resilience Hub exibirá Otimizar para regiãoRTO/RPOnas opções recomendadas. Se as metas regionais RTO e as RPO metas não estiverem definidas, a opção Otimizar para Zona de Disponibilidade (AZ)RTO/RPOserá exibida. Para obter mais informações sobre como definir RPO metas RTO regionais/ao criar políticas de resiliência, consulteCriar políticas de resiliência .
> - A carga de trabalho estimada RTO e RPO os valores estimados da carga de trabalho para os aplicativos e suas configurações são determinados considerando a quantidade de dados e o indivíduo. AppComponents No entanto, esses valores são apenas estimativas. Você deve usar seus próprios testes (como o Amazon Fault Injection Service) para testar seu aplicativo quanto aos tempos reais de recuperação.

Otimize para a zona de disponibilidadeRTO/RPO

Os menores tempos estimados possíveis de recuperação da carga de trabalho (RTO/RPO) durante uma interrupção na Zona de Disponibilidade (AZ). Se sua configuração não puder ser alterada o suficiente para atender às RPO metas RTO e, você será informado sobre os menores tempos estimados de recuperação da carga de trabalho AZ para que sua configuração se aproxime da possibilidade de atender à política.

Otimize para a regiãoRTO/RPO

Os menores tempos estimados possíveis de recuperação da carga de trabalho (RTO/RPO) durante uma interrupção regional. Se sua configuração não puder ser alterada o suficiente para atender às RPO metas RTO e, você será informado sobre os menores tempos estimados de recuperação da carga de trabalho na região para que sua configuração se aproxime da possibilidade de atender à política.

Otimizar para custo

O menor custo que você pode incorrer e ainda atender à sua política de resiliência. Se sua configuração não puder ser alterada o suficiente para atender às metas de otimização, você será informado sobre o menor custo possível para que sua configuração se aproxime da possibilidade de atender à política.

Otimizar para mudanças mínimas

As mudanças mínimas necessárias para atingir suas metas políticas. Se sua configuração não puder ser alterada o suficiente para atender às metas de otimização, você será informado sobre as mudanças recomendadas que podem aproximar sua configuração da possibilidade de cumprir a política.

Os itens a seguir estão incluídos nos detalhamentos da categoria de otimização:

- Descrição

  Descreve as configurações sugeridas por AWS Resilience Hub.
- Alterações

  Uma lista de alterações de texto que descrevem as tarefas necessárias para alternar para a configuração sugerida.
- Custo base

  O custo estimado associado às alterações recomendadas.

  > **Note**
  >
  > O custo base pode variar de acordo com o uso e não inclui descontos ou ofertas do Enterprise Discount Program (EDP).
- Carga de trabalho RTO estimada e RPO

  A carga de trabalho estimada RTO e a carga de trabalho estimada RPO após as mudanças.

AWSO Resilience Hub avalia se um componente de aplicativo (AppComponent) pode estar em conformidade com uma política de resiliência. Se o AppComponent não estiver em conformidade com uma política de resiliência e o AWS Resilience Hub não puder fazer nenhuma recomendação para facilitar a conformidade, pode ser porque o tempo de recuperação do selecionado AppComponent não pode ser atendido dentro das restrições do. AppComponent Exemplos de AppComponent restrições incluem tipo de recurso, tamanho do armazenamento ou configuração do recurso.

Para facilitar a conformidade AppComponent com a política de resiliência, altere o tipo de recurso AppComponent ou atualize a política de resiliência para se alinhar com o que o recurso pode oferecer.

Analisar recomendações operacionais

As recomendações operacionais contêm recomendações para configurar alarmes e AWS FIS experimentos por meio de AWS CloudFormation modelos. SOPs

AWS Resilience Hub fornece arquivos AWS CloudFormation de modelo para você baixar e gerenciar a infraestrutura do aplicativo como código. Como resultado, fornecemos recomendações no AWS CloudFormation para que você possa adicioná-las ao código do seu aplicativo. Se o tamanho do arquivo de AWS CloudFormation modelo for maior que um MB e contiver mais de 500 recursos, AWS Resilience Hub gera mais de um arquivo de AWS CloudFormation modelo em que o tamanho de cada arquivo não é maior que um MB e contém até 500 recursos. Se o arquivo de AWS CloudFormation modelo for dividido em vários arquivos, os nomes dos arquivos de AWS CloudFormation modelo serão acrescentados`partXofY`, o que `X` indica o número do arquivo na sequência e `Y` indica o número total de arquivos nos quais o arquivo de AWS CloudFormation modelo está dividido. Por exemplo, se o arquivo de modelo `big-app-template5-Alarm-104849185070-us-west-2.yaml` for dividido em quatro arquivos, os nomes dos arquivos serão os seguintes:

- `big-app-template5-Alarm-104849185070-us-west-2-part1of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part2of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part3of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part4of4.yaml`

No entanto, no caso de AWS CloudFormation modelos grandes, você deverá fornecer o Amazon Simple Storage Service URI em vez de usarCLI/APIcom o arquivo local como entrada.

Em AWS Resilience Hub, você pode realizar as seguintes ações:

- Você pode provisionar os alarmes e SOPs AWS FIS experimentos selecionados. Para provisionar alarmes e AWS FIS experimentos, selecione a recomendação apropriada e insira um nome exclusivo. SOPs AWS Resilience Hub cria um modelo com base nas recomendações selecionadas. Em Templates, você pode acessar seus modelos criados por meio de um Amazon Simple Storage Service (Amazon S3). URL
- Você pode incluir ou excluir alarmes e AWS FIS experimentos selecionados que foram recomendados para seu aplicativo a qualquer momento. SOPs Para obter mais informações, consulte, the section called “Incluir ou excluir recomendações operacionais”.

- Você também pode pesquisar, criar, adicionar, remover e gerenciar tags de um aplicativo e ver todas as tags associadas a ele.

Incluir ou excluir recomendações operacionais

AWS Resilience Hub fornece uma opção para incluir ou excluir os alarmes e SOPs os AWS FIS experimentos (testes) que foram recomendados para melhorar a pontuação de resiliência do seu aplicativo a qualquer momento. Incluir e excluir recomendações operacionais terá um impacto na pontuação de resiliência do seu aplicativo somente após a execução de uma nova avaliação. Portanto, recomendamos que você faça uma avaliação para obter a pontuação de resiliência atualizada e entender seu impacto em seu aplicativo.

Para obter mais informações sobre como restringir as permissões para incluir ou excluir recomendações por aplicativo, consulte the section called “Limitar as permissões para incluir ou excluir recomendações do AWS Resilience Hub ”.

Para incluir ou excluir recomendações operacionais de aplicativos

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Em Aplicativos, abra um aplicativo.
3. Escolha Avaliações e selecione uma avaliação na tabela de Avaliações de resiliência. Se você não tiver uma avaliação, conclua o procedimento em the section called “Executar avaliações de resiliência” e retorne a essa etapa.
4. Selecione a guia Recomendações operacionais.
5. Para incluir ou excluir recomendações operacionais do seu aplicativo, conclua as seguintes etapas:

Para incluir ou excluir alarmes recomendados do seu aplicativo

1. Para excluir alarmes, conclua as seguintes etapas:
    a. Na guia Alarmes, na tabela Alarmes, selecione todos os alarmes (com o estado Não implementado) que deseja excluir. Você pode identificar o estado atual de implementação de um alarme na coluna Estado.
    b. Em Ações, escolha Excluir selecionados.
    c. Na caixa de diálogo Excluir recomendações, selecione um dos seguintes motivos (opcional) e escolha Excluir selecionados para excluir os alarmes selecionados do aplicativo.

- Já implementado — Escolha essa opção se você já implementou esses alarmes em um AWS serviço como a Amazon CloudWatch ou qualquer outro provedor de serviços terceirizado.
- Não relevante: escolha esta opção se os alarmes não atenderem às suas necessidades comerciais.
- Muito complicado de implementar: escolha esta opção se você acha que esses alarmes são muito complicados de implementar.
- Outro: escolha esta opção para especificar qualquer outro motivo para excluir a recomendação.

2. Para incluir alarmes, conclua as seguintes etapas:

   a. Na guia Alarmes, na tabela Alarmes, selecione todos os alarmes (com estado Excluído) que deseja incluir. Você pode identificar o estado atual de implementação do alarme na coluna Estado.

   b. Em Ações, escolha Incluir selecionado.

   c. Na caixa de diálogo Incluir recomendações, escolha Incluir selecionados para incluir todos os alarmes selecionados em seu aplicativo.

Para incluir ou excluir procedimentos operacionais padrão recomendados (SOPs) do seu aplicativo

1. Para excluir o recomendadoSOPs, conclua as seguintes etapas:

   a. Na guia Procedimentos operacionais padrão, na SOPstabela, selecione todos os SOPs (com estado Implementado ou Não implementado) que você deseja excluir. Você pode identificar o estado atual de implementação SOP de an na coluna Estado.

   b. Em Ações, escolha Excluir selecionado para excluir o selecionado SOPs do seu aplicativo.

   c. Na caixa de diálogo Excluir recomendações, selecione um dos seguintes motivos (opcional) e escolha Excluir selecionado para excluir o selecionado SOPs do aplicativo.

      - Já implementado — Escolha essa opção se você já as implementou SOPs em um AWS serviço ou em qualquer outro provedor de serviços terceirizado.
      - Não relevante — Escolha essa opção se ela SOPs não atender às suas necessidades comerciais.
      - Muito complicado de implementar — Escolha essa opção se você acha que elas SOPs são muito complicadas de implementar.

- Nenhum: escolha esta opção se não quiser especificar o motivo.

2. Para incluirSOPs, conclua as seguintes etapas:

   a. Na guia Procedimentos operacionais padrão, na SOPstabela, selecione todos os alarmes (com estado excluído) que você deseja incluir. Você pode identificar o estado atual de implementação do alarme na coluna Estado.
   b. Em Ações, escolha Incluir selecionado.
   c. Na caixa de diálogo Incluir recomendações, escolha Incluir selecionados para incluir todos os selecionados SOPs em seu aplicativo.

Para incluir ou excluir testes recomendados do seu aplicativo

1. Para excluir os testes recomendados, conclua as seguintes etapas:

   a. Na guia Modelos de experimento de injeção de falhas, na tabela Modelos de experimento de injeção de falhas, selecione todos os testes (com estado Implementado ou Não implementado) que deseja excluir. Você pode identificar o estado atual de implementação de um teste na coluna Estado.
   b. Em Ações, escolha Excluir selecionados.
   c. Na caixa de diálogo Excluir recomendações, selecione um dos seguintes motivos (opcional) e escolha Excluir selecionados para excluir os experimentos do AWS FIS selecionados do aplicativo.

      - Já implementado — Escolha essa opção se você já implementou esses testes em um AWS serviço ou em qualquer outro provedor de serviços terceirizado.
      - Não relevante: escolha esta opção se os testes não atenderem às suas necessidades comerciais.
      - Muito complicado de implementar: escolha esta opção se você acha que esses testes são muito complicados de implementar.
      - Nenhum: escolha esta opção se não quiser especificar o motivo.

2. Para incluir os testes recomendados, conclua as seguintes etapas:

   a. Na guia Modelos de experimento de injeção de falhas, na tabela Modelos de experimento de injeção de falhas, selecione todos os testes (com estado Excluído) que deseja incluir. Você pode identificar o estado atual de implementação do teste na coluna Estado.
   b. Em Ações, escolha Incluir selecionado.

c. Na caixa de diálogo Incluir recomendações, escolha Incluir selecionados para incluir todos os testes selecionados em seu aplicativo.

Excluir avaliações de resiliência

Você pode excluir avaliações de resiliência na exibição Avaliações do seu aplicativo.

Para excluir uma avaliação de resiliência

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Em Aplicativos, abra um aplicativo.
3. Em Avaliações, escolha um relatório de avaliação na tabela Avaliações de resiliência.
4. Para confirmar a exclusão, selecione Excluir.

   O relatório não aparece mais na tabela Avaliações de resiliência.

Gerenciar alarmes

Quando você executa uma avaliação de resiliência, como parte das recomendações operacionais, AWS Resilience Hub recomenda configurar CloudWatch alarmes da Amazon para monitorar a resiliência do seu aplicativo. Recomendamos esses alarmes com base nos recursos e componentes da configuração atual do aplicativo. Se os recursos e componentes do seu aplicativo mudarem, você deverá executar uma avaliação de resiliência para garantir que tenha os alarmes corretos para o aplicativo atualizado.

AWS Resilience Hub fornece um arquivo de modelo (`README.md`) que permite criar alarmes recomendados por AWS Resilience Hub dentro AWS (como a Amazon CloudWatch) ou por fora AWS. Os valores padrão fornecidos nos alarmes são baseados nas melhores práticas usadas para criar esses alarmes.

Tópicos

Criação de alarmes a partir das recomendações operacionais

AWS Resilience Hub cria um AWS CloudFormation modelo que contém detalhes para criar os alarmes selecionados na Amazon CloudWatch. Depois que o modelo for gerado, você poderá acessá-lo por meio de um Amazon S3URL, fazer o download do mesmo e colocá-lo em seu pipeline de código ou criar uma pilha por meio do console. AWS CloudFormation

Para criar um alarme com base nas AWS Resilience Hub recomendações, você deve criar um AWS CloudFormation modelo para os alarmes recomendados e incluí-los na sua base de código.

Para criar alarmes nas recomendações operacionais

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Em Aplicativos, escolha seu aplicativo.
3. Escolha a guia Avaliações.

   Na tabela Avaliações de resiliência, você pode identificar suas avaliações usando as seguintes informações:

   - Nome: nome da avaliação que você forneceu no momento da criação.
   - Status: indica o estado de execução da avaliação.
   - Status de conformidade: indica se a avaliação está em conformidade com a política de resiliência.
   - Status de desvio de resiliência: indica se seu aplicativo se desviou ou não da avaliação anterior bem-sucedida.
   - Versão do aplicativo: versão do seu aplicativo.
   - Invocador: indica a função que invocou a avaliação.
   - Horário de início: indica o horário de início da avaliação.
   - Horário de término: indica o horário de término da avaliação.
   - ARN— O nome do recurso Amazon (ARN) da avaliação.
4. Selecione uma avaliação na tabela Avaliações de resiliência. Se você não tiver uma avaliação, conclua o procedimento em the section called “Executar avaliações de resiliência” e retorne a essa etapa.
5. Escolha Recomendações operacionais.
6. Se não estiver selecionado por padrão, escolha a guia Alarmes.

Na tabela Alarmes, você pode identificar os alarmes recomendados usando o seguinte:

- Nome: nome do alarme que você definiu para seu aplicativo.
- Descrição: descreve o objetivo do alarme.
- Estado — Indica o estado atual de implementação dos CloudWatch alarmes da Amazon.

  Essa coluna exibe um dos valores a seguir:

  - Implementado — Indica que os alarmes recomendados pelo AWS Resilience Hub estão implementados em seu aplicativo. A escolha do número abaixo filtrará a tabela Alarmes para exibir todos os alarmes recomendados que são implementados em seu aplicativo.
  - Não implementado — Indica que os alarmes recomendados pelo AWS Resilience Hub estão incluídos, mas não foram implementados em seu aplicativo. A escolha do número abaixo filtrará a tabela Alarmes para exibir todos os alarmes recomendados que não estão implementados em seu aplicativo.
  - Excluído — Indica que os alarmes recomendados pelo foram AWS Resilience Hub excluídos do seu aplicativo. A escolha do número abaixo filtrará a tabela Alarmes para exibir todos os alarmes recomendados que foram excluídos do seu aplicativo. Para obter mais informações sobre como incluir e excluir alarmes recomendados, consulte Incluir ou excluir recomendações operacionais.
  - Inativo — Indica que os alarmes foram implantados na Amazon CloudWatch, mas o status está definido como _ INSUFFICIENTna DATA Amazon. CloudWatch A escolha do número abaixo filtrará a tabela Alarmes para exibir todos os alarmes implementados e inativos.
- Configuração: indica se há alguma dependência de configuração pendente que precisa ser abordada.
- Tipo: indica o tipo de alarme.
- AppComponent— Indica os componentes do aplicativo (AppComponents) associados a esse alarme.
- ID de referência — Indica o identificador lógico do evento de AWS CloudFormation pilha em AWS CloudFormation.
- ID de recomendação — Indica o identificador lógico do recurso de AWS CloudFormation pilha em AWS CloudFormation.

7. Na guia Alarmes, para filtrar as recomendações na tabela Alarmes com base em um estado específico, selecione um número abaixo do mesmo.

8. Selecione os alarmes recomendados que você deseja configurar para seu aplicativo e escolha Criar CloudFormation modelo.
9. Na caixa CloudFormation de diálogo Criar modelo, você pode usar o nome gerado automaticamente ou inserir um nome para o AWS CloudFormation modelo na caixa de nome do CloudFormation modelo.
10. Escolha Criar. Isso pode levar alguns minutos para criar o AWS CloudFormation modelo.

    Conclua o procedimento a seguir para incluir as recomendações em sua base de código.

Para incluir as AWS Resilience Hub recomendações, sua base de código

1. Escolha a guia Modelos para ver o modelo que você acabou de criar. Você pode identificar seus modelos usando o seguinte:
   - Nome: nome da avaliação que você forneceu no momento da criação.
   - Status: indica o estado de execução da avaliação.
   - Tipo: indica o tipo de recomendação operacional.
   - Formato — Indica o formato (JSON/texto) no qual o modelo é criado.
   - Horário de início: indica o horário de início da avaliação.
   - Horário de término: indica o horário de término da avaliação.
   - ARN— O ARN do modelo
2. Em Detalhes do modelo, escolha o link em Caminho do S3 dos modelos para abrir o objeto de modelo no console do Amazon S3.
3. No console do Amazon S3, na tabela Objetos, escolha o link da SOP pasta.
4. Para copiar o caminho do Amazon S3, marque a caixa de seleção na frente do JSON arquivo e escolha Copiar. URL
5. Crie uma AWS CloudFormation pilha a partir do AWS CloudFormation console. Para obter mais informações sobre como criar uma AWS CloudFormation pilha, consultehttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Ao criar a AWS CloudFormation pilha, você deve fornecer o caminho do Amazon S3 que você copiou da etapa anterior.

Visualizar alarmes

Você pode visualizar todos os alarmes ativos que você configurou para monitorar a resiliência de seus aplicativos. AWS Resilience Hub usa o AWS CloudFormation modelo para armazenar detalhes do alarme que, por sua vez, são usados para criar os alarmes na Amazon. CloudWatch Você pode acessar o AWS CloudFormation modelo usando o Amazon S3URL, baixá-lo e colocá-lo em seu pipeline de código ou criar uma pilha por meio do console. AWS CloudFormation

Para visualizar os alarmes no painel, escolha Painel no menu de navegação esquerdo. Na tabela de alarmes implementados, você pode identificar os alarmes implementados usando as seguintes informações:

- Aplicativo afetado: nome dos aplicativos que implementaram esse alarme.
- Alarmes ativos: indica o número de alarmes ativos acionados pelos aplicativos.
- FISem andamento — Indica o AWS FIS experimento que está sendo executado no momento para seu aplicativo.

Para visualizar os alarmes implementados em seu aplicativo

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Selecione um aplicativo na tabela Aplicativos.
3. Na página de resumo do aplicativo, a tabela Alarmes implementados exibe todos os alarmes recomendados que são implementados em seu aplicativo.

   Para localizar um alarme específico na tabela Alarmes implementados, na caixa Localizar alarmes por texto, propriedade ou valor, selecione um dos seguintes campos, escolha uma operação e digite um valor.

   - Nome do alarme: nome do alarme que você definiu para seu aplicativo.
   - Descrição: descreve o objetivo do alarme.
   - Estado — Indica o estado atual de implementação do CloudWatch alarme da Amazon.

     Essa coluna exibe um dos valores a seguir:

     - Implementado — Indica que os alarmes recomendados pelo AWS Resilience Hub estão implementados em seu aplicativo. Escolha o número abaixo para ver todos os alarmes recomendados e implementados na guia Recomendações operacionais.

- Não implementado — Indica que os alarmes recomendados pelo AWS Resilience Hub estão incluídos, mas não foram implementados em seu aplicativo. Escolha o número abaixo para ver todos os alarmes recomendados e não implementados na guia Recomendações operacionais.
- Excluído — Indica que os alarmes recomendados pelo foram AWS Resilience Hub excluídos do seu aplicativo. Escolha o número abaixo para ver todos os alarmes recomendados e excluídos na guia Recomendações operacionais. Para obter mais informações sobre como incluir e excluir alarmes recomendados, consulte Incluir ou excluir recomendações operacionais.
- Inativo — Indica que os alarmes foram implantados na Amazon CloudWatch, mas o status está definido como _ INSUFFICIENTna DATA Amazon. CloudWatch Escolha o número abaixo para ver todos os alarmes implementados e inativos na guia Recomendações operacionais.

- Modelo de origem — Fornece o Amazon Resource Name (ARN) da AWS CloudFormation pilha que contém os detalhes do alarme.
- Recurso: exibe os recursos aos quais esse alarme está anexado e para os quais foi implementado.
- Métrica — Exibe a CloudWatch métrica da Amazon atribuída ao alarme. Para obter mais informações sobre as CloudWatch métricas da Amazon, consulte Amazon CloudWatch Metrics.
- Última alteração: exibe a data e a hora em que um alarme foi modificado pela última vez.

Para visualizar os alarmes recomendados nas avaliações

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Selecione um aplicativo na tabela Aplicativos.

   Para localizar um aplicativo, insira o nome do aplicativo na caixa Localizar aplicativos.
3. Escolha a guia Avaliações.

   Na tabela Avaliações de resiliência, você pode identificar suas avaliações usando as seguintes informações:

   - Nome: nome da avaliação que você forneceu no momento da criação.
   - Status: indica o estado de execução da avaliação.

- Status de conformidade: indica se a avaliação está em conformidade com a política de resiliência.
- Status de desvio de resiliência: indica se seu aplicativo se desviou ou não da avaliação anterior bem-sucedida.
- Versão do aplicativo: versão do seu aplicativo.
- Invocador: indica a função que invocou a avaliação.
- Horário de início: indica o horário de início da avaliação.
- Horário de término: indica o horário de término da avaliação.
- ARN— O nome do recurso Amazon (ARN) da avaliação.

4. Selecione uma avaliação na tabela Avaliações de resiliência.
5. Escolha a guia Recomendações operacionais.
6. Se não estiver selecionado por padrão, escolha a guia Alarmes.

   Na tabela Alarmes, você pode identificar os alarmes recomendados usando o seguinte:

   - Nome: nome do alarme que você definiu para seu aplicativo.
   - Descrição: descreve o objetivo do alarme.
   - Estado — Indica o estado atual de implementação dos CloudWatch alarmes da Amazon.

     Essa coluna exibe um dos valores a seguir:

     - Implementado: indica que o alarme foi implementado em seu aplicativo. A escolha do número abaixo filtrará a tabela Alarmes para exibir todos os alarmes recomendados que são implementados em seu aplicativo.
     - Não implementado: indica que o alarme não foi implementado ou incluído em seu aplicativo. A escolha do número abaixo filtrará a tabela Alarmes para exibir todos os alarmes recomendados que não estão implementados em seu aplicativo.
     - Excluído: indica que o alarme foi excluído do aplicativo. A escolha do número abaixo filtrará a tabela Alarmes para exibir todos os alarmes recomendados que foram excluídos do seu aplicativo. Para obter mais informações sobre como incluir e excluir alarmes recomendados, consulte the section called “Incluir ou excluir recomendações operacionais”.
     - Inativo — Indica que os alarmes foram implantados na Amazon CloudWatch, mas o status está definido como _ INSUFFICIENTna DATA Amazon. CloudWatch A escolha do número abaixo filtrará a tabela Alarmes para exibir todos os alarmes implementados e inativos.

- Configuração: indica se há alguma dependência de configuração pendente que precisa ser abordada.
- Tipo: indica o tipo de alarme.
- AppComponent— Indica os componentes do aplicativo (AppComponents) associados a esse alarme.
- ID de referência — Indica o identificador lógico do evento de AWS CloudFormation pilha em AWS CloudFormation.
- ID de recomendação — Indica o identificador lógico do recurso de AWS CloudFormation pilha em AWS CloudFormation.

Gerenciando procedimentos operacionais padrão

Um procedimento operacional padrão (SOP) é um conjunto prescritivo de etapas projetado para recuperar seu aplicativo com eficiência no caso de uma interrupção ou alarme. Prepare, teste e meça seus SOPs com antecedência para garantir uma recuperação oportuna no caso de uma interrupção operacional.

Com base nos componentes do seu aplicativo, AWS Resilience Hub recomenda os SOPs que você deve preparar. AWS Resilience Hub trabalha com o Systems Manager para automatizar as etapas de seus SOPs, fornecendo vários documentos SSM que você pode usar como base para esses SOPs.

Por exemplo, AWS Resilience Hub pode recomendar um SOP para adicionar espaço em disco com base em um documento de automação SSM existente. Para executar esse documento SSM, você precisa de uma função específica do IAM com as permissões corretas. AWS Resilience Hub cria metadados em seu aplicativo indicando qual documento de automação de SSM executar em caso de falta de disco e qual função do IAM é necessária para executar esse documento de SSM. Esses metadados são então salvos em um parâmetro do SSM.

Além de configurar a automação do SSM, também é uma prática recomendada testá-la com um experimento do AWS FIS . Portanto, AWS Resilience Hub também fornece um AWS FIS experimento que chama o documento de automação do SSM. Dessa forma, você pode testar proativamente seu aplicativo para garantir que o SOP que você criou faça o trabalho pretendido.

AWS Resilience Hub fornece suas recomendações na forma de um AWS CloudFormation modelo que você pode adicionar à base de código do seu aplicativo. Esse modelo fornece:

- Um perfil do IAM com as permissões necessárias para executar o SOP.
- Um AWS FIS experimento que você pode usar para testar o SOP.
- Um parâmetro do SSM que contém metadados do aplicativo indicando qual documento do SSM e qual perfil do IAM devem ser executados como SOP e em qual recurso. Por exemplo: `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`.

Criar um SOP pode exigir algumas tentativas e erros. Executar uma avaliação de resiliência em relação ao seu aplicativo e gerar um AWS CloudFormation modelo a partir das AWS Resilience Hub recomendações é um bom começo. Use o AWS CloudFormation modelo para gerar uma AWS CloudFormation pilha e, em seguida, use os parâmetros SSM e seus valores padrão em seu SOP. Execute o SOP e veja quais refinamentos você precisa fazer.

Como todos os aplicativos têm requisitos diferentes, a lista padrão de documentos do SSM que o AWS Resilience Hub fornece não será suficiente para todas as suas necessidades. No entanto, você pode copiar os documentos do SSM padrão e usá-los como base para criar seus próprios documentos personalizados para seu aplicativo. Você também pode criar seus próprios documentos do SSM completamente novos. Se você criar seus próprios documentos do SSM em vez de modificar os padrões, deverá associá-los aos parâmetros do SSM, para que o documento do SSM correto seja chamado quando o SOP for executado.

Depois de finalizar seu SOP criando os documentos do SSM necessários e atualizando as associações de parâmetros e documentos conforme necessário, adicione os documentos do SSM diretamente à sua base de código e faça as alterações ou personalizações subsequentes lá. Dessa forma, toda vez que você implantar seu aplicativo, você também implantará a maior parte do up-to-date SOP.

Tópicos

Construindo um SOP com base em recomendações AWS Resilience Hub

Para criar um SOP com base em AWS Resilience Hub recomendações, você precisa de um AWS Resilience Hub aplicativo com uma política de resiliência anexada a ele e precisa ter executado uma avaliação de resiliência em relação a esse aplicativo. A avaliação de resiliência gera as recomendações para seu SOP.

Para criar um SOP com base em AWS Resilience Hub recomendações, você deve criar um AWS CloudFormation modelo para os SOPs recomendados e incluí-los em sua base de código.

Crie um AWS CloudFormation modelo para as recomendações do SOP

1. Abra o AWS Resilience Hub console.
2. No painel de navegação, escolha Aplicativos.
3. Na lista de aplicativos, escolha o aplicativo para o qual você deseja criar um SOP.
4. Escolha a guia Avaliações.
5. Selecione uma avaliação na tabela Avaliações de resiliência. Se você não tiver uma avaliação, conclua o procedimento em the section called “Executar avaliações de resiliência” e retorne a essa etapa.
6. Em Recomendações operacionais, escolha Procedimentos operacionais padrão.
7. Selecione todas as recomendações do SOP que deseja incluir.
8. Escolha Criar CloudFormation modelo. Isso pode levar alguns minutos para criar o AWS CloudFormation modelo.

   Conclua o procedimento a seguir para incluir as recomendações do SOP em sua base de código.

Para incluir as AWS Resilience Hub recomendações em sua base de código

1. Em Recomendações operacionais, escolha Modelos.
2. Na lista de modelos, escolha o nome do modelo do SOP que você acabou de criar.

   Você pode identificar os SOPs que são implementados em seu aplicativo usando as seguintes informações:

   - Nome do SOP: nome do SOP que você definiu para seu aplicativo.
   - Descrição: descreve o objetivo do SOP.

- Documento do SSM: URL do Amazon S3 do documento do SSM que contém a definição do SOP.
- Execução de teste: URL do Amazon S3 do documento que contém os resultados do teste mais recente.
- Modelo de origem — fornece o nome de recurso da Amazon (ARN) da AWS CloudFormation pilha que contém os detalhes do SOP.

3. Em Detalhes do modelo, escolha o link em Caminho do S3 dos modelos para abrir o objeto de modelo no console do Amazon S3.
4. No console do Amazon S3, na tabela Objetos, escolha o link da pasta SOP.
5. Para copiar o caminho do Amazon S3, marque a caixa de seleção na frente do arquivo JSON e escolha Copiar URL.
6. Crie uma AWS CloudFormation pilha a partir do AWS CloudFormation console. Para obter mais informações sobre como criar uma pilha do AWS CloudFormation , consulte https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Ao criar a AWS CloudFormation pilha, você deve fornecer o caminho do Amazon S3 que você copiou da etapa anterior.

Criar um documento do SSM personalizado

Para automatizar totalmente a recuperação do seu aplicativo, talvez seja necessário criar um documento do SSM personalizado para seu SOP no console do Systems Manager. Você pode modificar um documento do SSM existente como base ou criar um novo documento do SSM.

Para obter informações detalhadas sobre o uso do Systems Manager para criar um documento do SSM, consulte Passo a passo: Uso do Document Builder para criar um runbook personalizado.

Para obter informações sobre a sintaxe de documento do SSM, consulte Sintaxe de documento do SSM.

Para obter informações sobre a automatização das ações do documento do SSM, consulte Referência de ações de automação do Systems Manager.

Usar um documento do SSM personalizado em vez do padrão

Para substituir o documento SSM AWS Resilience Hub sugerido para seu SOP por um documento personalizado que você criou, trabalhe diretamente em sua base de código. Além de adicionar seu novo documento personalizado de automação do SSM, você também vai:

1. Adicionar as permissões do IAM necessárias para executar a automação.
2. Adicione um AWS FIS experimento para testar seu documento SSM.
3. Adicionar um parâmetro do SSM que aponte para o documento de automação que você deseja usar como SOP.

Geralmente, é mais eficiente trabalhar com os valores padrão sugeridos AWS Resilience Hub e personalizá-los conforme necessário. Por exemplo, adicione ou remova permissões conforme necessário para a função do IAM, altere a configuração do AWS FIS experimento para apontar para o novo documento SSM ou altere o parâmetro SSM para apontar para seu novo documento SSM.

Teste de SOPs

Conforme mencionado anteriormente, a melhor prática é adicionar AWS FIS experimentos aos seus pipelines de CI/CD para testar seus SOPs regularmente; isso garante que eles estejam prontos para uso caso ocorra uma interrupção.

Teste os AWS Resilience Hub SOPs fornecidos e personalizados.

Visualizar procedimentos operacionais padrão

Para visualizar os SOPs implementados a partir dos aplicativos

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Em Aplicativos, abra um aplicativo.
3. Escolha a guia Procedimentos operacionais padrão.

   Na seção Resumo dos procedimentos operacionais padrão, a tabela Procedimentos operacionais padrão implementados exibe a lista de SOPs que são gerados a partir das recomendações de SOP.

   Você pode identificar seus SOPs da seguinte forma:

- Nome do SOP: nome do SOP que você definiu para seu aplicativo.
- Documento do SSM: URL do S3 do documento do Amazon EC2 Systems Manager que contém a definição do SOP.
- Descrição: descreve o objetivo do SOP.
- Execução do teste: URL do S3 do documento que contém os resultados do teste mais recente.
- ID de referência: identificador da recomendação de SOP referenciada.
- ID do recurso: identificador do recurso para o qual a recomendação do SOP é implementada.

Para visualizar os SOPs recomendados nas avaliações

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Selecione um aplicativo na tabela Aplicativos.

   Para localizar um aplicativo, insira o nome do aplicativo na caixa Localizar aplicativos.
3. Escolha a guia Avaliações.

   Na tabela Avaliações de resiliência, você pode identificar suas avaliações usando as seguintes informações:

   - Nome: nome da avaliação que você forneceu no momento da criação.
   - Status: indica o estado de execução da avaliação.
   - Status de conformidade: indica se a avaliação está em conformidade com a política de resiliência.
   - Status de desvio de resiliência: indica se seu aplicativo se desviou ou não da avaliação anterior bem-sucedida.
   - Versão do aplicativo: versão do seu aplicativo.
   - Invocador: indica a função que invocou a avaliação.
   - Horário de início: indica o horário de início da avaliação.
   - Horário de término: indica o horário de término da avaliação.
   - ARN: o nome do recurso da Amazon (ARN) da avaliação.
4. Selecione uma avaliação na tabela Avaliações de resiliência.
5. Escolha a guia Recomendações operacionais.

6. Escolha a guia Procedimentos operacionais padrão.

   Na tabela de Procedimentos operacionais padrão, você pode entender mais sobre os SOPs recomendados usando as seguintes informações:

   - Nome: nome do SOP recomendado.
   - Descrição: descreve o objetivo do SOP.
   - Estado: indica o estado atual de implementação do SOP. Ou seja, Implementado, Não implementado e Excluído.
   - Configuração: indica se há alguma dependência de configuração pendente que precisa ser abordada.
   - Tipo: indica o tipo de SOP.
   - AppComponent— Indica os componentes do aplicativo (AppComponents) associados a esse SOP. Para obter mais informações sobre o suporte AppComponents, consulte Agrupando recursos em um AppComponent.
   - ID de referência — Indica o identificador lógico do evento de AWS CloudFormation pilha em AWS CloudFormation.
   - ID da recomendação: indica o identificador lógico do recurso de pilha do AWS CloudFormation no AWS CloudFormation.

Gerenciando experimentos do Amazon Fault Injection Service

Esta seção descreve como criar e executar experimentos do Amazon Fault Injection Service (AWS FIS) no AWS Resilience Hub. Você realiza AWS FIS experimentos para medir a resiliência de seus AWS recursos e o tempo necessário para se recuperar do aplicativo, da infraestrutura, da zona de disponibilidade e dos Região da AWS incidentes.

Para medir a resiliência, esses AWS FIS experimentos simulam interrupções em seus recursos. AWS Exemplos de interrupções incluem erros de rede indisponível, failovers, processos interrompidos no Amazon EC2 ou AWS ASG, recuperação de inicialização no Amazon RDS e problemas com sua zona de disponibilidade. Quando o AWS FIS experimento for concluído, você poderá estimar se um aplicativo pode se recuperar dos tipos de interrupção definidos na meta de RTO da política de resiliência.

Todos os experimentos AWS Resilience Hub são construídos usando AWS FIS e executam AWS FIS ações. A maioria dos AWS FIS experimentos invoca ações de automação do Systems Manager

para realizar interrupções e monitorar os alarmes, e outros AWS FIS experimentos usam somente ações de AWS FIS automação personalizadas para AWS serviços específicos (como a ação do Amazon EKS). Para obter mais informações sobre ações do AWS FIS , consulte AWS FIS referência de ações.

Você pode usar os AWS FIS experimentos em seu estado padrão ou personalizá-los com base em seus requisitos. AWS FIS os experimentos podem ser acessados a partir de AWS Resilience Hub (the section called “Visualizar experimentos de injeção de falhas”) ou AWS FIS console (AWS FIS).

Tópicos

Criando AWS FIS experimentos a partir das recomendações operacionais

AWS Resilience Hub recomenda que você teste seu aplicativo depois de executar um relatório de avaliação. Você pode acessar e executar esses experimentos a partir do relatório de avaliação do seu aplicativo.

AWS Resilience Hub fornece uma lista de AWS FIS experimentos, que são documentos do Systems Manager com parâmetros de teste. Quando você seleciona um AWS FIS experimento na lista, AWS Resilience Hub cria um AWS CloudFormation modelo com os parâmetros definidos no documento Systems Manager. Após a criação da AWS CloudFormation pilha, você pode ver seus AWS FIS experimentos provisionados para seu aplicativo.

O AWS CloudFormation modelo consiste em uma função do IAM para cada documento do Systems Manager, com as permissões mínimas necessárias para execução.

Para criar um AWS FIS experimento com base em AWS Resilience Hub recomendações, você deve criar um AWS CloudFormation modelo para os testes recomendados e incluí-los em sua base de código.

Para criar um AWS CloudFormation modelo para o AWS FIS experimento

1. Abra o AWS Resilience Hub console.

2. No painel de navegação, escolha Aplicativos.
3. Na lista de aplicativos, escolha o aplicativo para o qual você deseja criar um teste.
4. Escolha a guia Avaliações.
5. Selecione uma avaliação na tabela Avaliações de resiliência. Se você não tiver uma avaliação, conclua o procedimento em the section called “Executar avaliações de resiliência” e retorne a essa etapa.
6. Em Recomendações operacionais, escolha Experimentos de injeção de falhas.
7. Selecione todos os testes que deseja incluir.
8. Escolha Criar CloudFormation modelo. Isso pode levar alguns minutos para criar o AWS CloudFormation modelo.
9. Escolha Modelos.

   Você pode ver o AWS CloudFormation modelo recém-criado na tabela Modelos.

   Conclua o procedimento a seguir para incluir as recomendações em sua base de código.

Para incluir as AWS Resilience Hub recomendações em sua base de código

1. Em Recomendações operacionais, escolha Modelos.
2. Na lista de modelos, escolha o nome do modelo de AWS FIS experimento que você acabou de criar.

   Você pode identificar os testes que são implementados em seu aplicativo usando as seguintes informações:

   - Nome do teste: nome do teste que você criou para seu aplicativo.
   - Descrição: descreve o objetivo do teste.
   - Estado: indica o estado atual de implementação do teste.

     Essa coluna exibe um dos valores a seguir:

     - Implementado: indica que o teste foi implementado em seu aplicativo.
     - Não implementado: indica que o teste não foi implementado ou incluído em seu aplicativo.
     - Excluído: indica que o teste foi excluído do aplicativo.
     - Inativo — Indica que o teste foi implantado AWS FIS, mas não foi executado nos últimos 30 dias.

- Execução de teste: URL do Amazon S3 do documento que contém os resultados do teste mais recente.
- Modelo de origem — fornece o nome de recurso da Amazon (ARN) da AWS CloudFormation pilha que contém os detalhes do experimento.

3. Em Detalhes do modelo, escolha o link em Caminho dos modelos do S3 para abrir o objeto de modelo no console do Amazon S3.
4. No console do Amazon S3, na tabela Objetos, escolha o link da pasta de teste.
5. Para copiar o caminho do Amazon S3, marque a caixa de seleção na frente do arquivo JSON e escolha Copiar URL.
6. Crie uma AWS CloudFormation pilha a partir do AWS CloudFormation console. Para obter mais informações sobre como criar uma AWS CloudFormation pilha, consulte https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Ao criar a AWS CloudFormation pilha, você deve fornecer o caminho do Amazon S3 que você copiou da etapa anterior.

Executando um AWS FIS experimento a partir de AWS Resilience Hub

Em seu aplicativo, você deve primeiro criar um modelo de AWS FIS experimento a partir das recomendações operacionais antes de AWS Resilience Hub poder executar o AWS FIS experimento.

Para começar um AWS FIS experimento

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Na tabela Aplicativos, abra um aplicativo.
3. Escolha a guia Experimentos de injeção de falhas.
4. Selecione o botão de opções antes do modelo de experimento usado para criar o experimento que deseja executar na tabela Modelos de experimento e, em seguida, escolha Iniciar experimento.

Para interromper um AWS FIS experimento

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Na tabela Aplicativos, abra um aplicativo.
3. Escolha a guia Experimentos de injeção de falhas.

4. Selecione o botão de opções antes do experimento na tabela Experimento e, em seguida, escolha Interromper experimento.

Visualizar experimentos de injeção de falhas

Em AWS Resilience Hub, visualize os AWS FIS experimentos que você configurou para medir a resiliência de seus AWS recursos e o tempo necessário para se recuperar do aplicativo, da infraestrutura, da zona de disponibilidade e dos Região da AWS incidentes.

Para ver AWS FIS os experimentos no painel, escolha Painel no menu de navegação à esquerda. Na tabela Experimentos, você pode identificar os AWS FIS experimentos implementados usando as seguintes informações:

- ID do experimento: identificador do experimento do AWS FIS .
- ID do modelo de AWS FIS experimento — Identificador do modelo de experimento usado para criar o AWS FIS experimento.
- Modelo de origem — fornece o Amazon Resource Name (ARN) da AWS CloudFormation pilha que contém detalhes do experimento. AWS FIS
- Estado — Indica se o AWS FIS experimento foi concluído com sucesso ou não.

Para visualizar os AWS FIS experimentos implementados a partir de aplicativos

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Na tabela Aplicativos, abra um aplicativo.
3. Escolha Experimentos de injeção de falhas.
4. Escolha a guia Experimento.

   Na guia Experiência, você pode ver uma lista de AWS FIS experiências ativas na tabela Experiência.

   Na tabela Experimentos, você pode identificar o experimento do AWS FIS implementado usando as seguintes informações:

   - Nome do teste — Nome do teste recomendado pelo AWS Resilience Hub que foi usado para criar o AWS FIS experimento.
   - ID do experimento: identificador do experimento do AWS FIS .

- Descrição — Descreve o objetivo do AWS FIS experimento.
- Hora de criação: data e hora em que o experimento do AWS FIS foi criado.
- Hora da última atualização: data e hora em que o experimento do AWS FIS foi atualizado pela última vez.
- Modelo de origem — fornece o Amazon Resource Name (ARN) da AWS CloudFormation pilha que contém detalhes do experimento. AWS FIS

Visualizar os experimentos recomendados a partir das avaliações

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Selecione um aplicativo na tabela Aplicativos.

   Para localizar um aplicativo, insira o nome do aplicativo na caixa Localizar aplicativos.
3. Escolha a guia Avaliações.

   Na tabela Avaliações de resiliência, você pode identificar suas avaliações usando as seguintes informações:

   - Nome: nome da avaliação que você forneceu no momento da criação.
   - Status: indica o estado de execução da avaliação.
   - Status de conformidade: indica se a avaliação está em conformidade com a política de resiliência.
   - Status de desvio de resiliência: indica se seu aplicativo se desviou ou não da avaliação anterior bem-sucedida.
   - Versão do aplicativo: versão do seu aplicativo.
   - Invocador: indica a função que invocou a avaliação.
   - Horário de início: indica o horário de início da avaliação.
   - Horário de término: indica o horário de término da avaliação.
   - ARN: o nome do recurso da Amazon (ARN) da avaliação.
4. Selecione uma avaliação na tabela Avaliações de resiliência.
5. Escolha a guia Recomendações operacionais.
6. Escolha a guia Experimentos de injeção de falhas.

Na tabela Modelos de experimentos de injeção de falhas, você pode entender mais sobre os testes recomendados usando as seguintes informações:

- Nome: nome do teste recomendado.
- Descrição: descreve o objetivo do teste.
- Estado: indica o estado atual de implementação do teste.

  Essa coluna exibe um dos valores a seguir:

  - Implementado: indica que o teste foi implementado em seu aplicativo.
  - Não implementado: indica que o teste não foi implementado ou incluído em seu aplicativo.
  - Excluído: indica que o teste foi excluído do aplicativo.
  - Inativo — Indica que o teste foi implantado AWS FIS, mas não foi executado nos últimos 30 dias.
- Configuração: indica se há alguma dependência de configuração pendente que precisa ser abordada.
- Tipo: indica o tipo de teste.
- AppComponent— Indica os componentes do aplicativo (AppComponents) associados a esse teste. Para obter mais informações sobre o suporte AppComponents, consulte Agrupando recursos em um AppComponent.
- Risco: indica o nível de risco da falha do teste. Os níveis de risco são indicados usando Alto, Médio e Baixo para indicar níveis de risco alto, moderado e baixo, respectivamente.
- ID de referência — Indica o identificador lógico do evento de AWS CloudFormation pilha em AWS CloudFormation.
- ID de recomendação — Indica o identificador lógico do recurso de AWS CloudFormation pilha em AWS CloudFormation.

Verificação de falhas/status do experimento do Amazon Fault Injection Service

AWS Resilience Hub permite que você acompanhe o status do experimento que você iniciou. Para obter mais informações, consulte o procedimento Visualizar os experimentos recomendados a partir das avaliações no the section called “Visualizar experimentos de injeção de falhas”.

Tópicos

- Analisando a execução do AWS FIS experimento usando o AWS Systems Manager
- AWS FIS falhas de experimentos ao testar pods do Kubernetes em execução em seus clusters do Amazon Elastic Kubernetes Service

Analisando a execução do AWS FIS experimento usando o AWS Systems Manager

Depois de realizar um AWS FIS experimento, você pode ver os detalhes da execução no AWS Systems Manager.

1. Vá até CloudTrail> Histórico de eventos.
2. Filtre os eventos por Nome de usuário usando o ID do experimento.
3. Veja a StartAutomationExecution entrada. O ID da solicitação é o ID de automação do SSM.
4. Acesse AWS Systems Manager > Automação.
5. Filtre por ID de execução usando o ID de automação do SSM e visualize os detalhes da automação.

   Você pode analisar a execução com qualquer automação do Systems Manager. Para obter mais informações, consulte o guia do usuário do AWS Systems Manager Automation. Os parâmetros de entrada da execução aparecem na seção Parâmetros de entrada do Detalhe da execução e incluem parâmetros opcionais que não aparecem no AWS FIS experimento.

   Você pode encontrar informações sobre o status e outros detalhes da etapa detalhando as etapas específicas nas etapas de execução.

Falhas comuns

Veja a seguir as falhas comuns encontradas durante a execução de um relatório de avaliação:

- O modelo de alarme não foi implantado antes da execução do experimento de teste/SOP. Isso causa uma mensagem de erro durante a etapa de automação.
  - Mensagem de falha: `The following parameters were not found: [/ResilienceHub/Alarm/3dee49a1-9877-452a-bb0c-a958479a8ef2/nat-gw-alarm-bytes-out-to-source-2020-09-21_nat-02ad9bc4fbd4e6135]. Make sure all the SSM parameters in automation document are created in SSM Parameter Store.`

  - Remediação: certifique-se de renderizar o alarme relevante e implantar o modelo resultante antes de executar novamente o experimento de injeção de falhas.
- Permissões ausentes na função de execução. Essa mensagem de erro ocorre se a função de execução fornecida não tiver uma permissão e aparecer nos detalhes da etapa.
  - Mensagem de falha: `An error occurred (Unauthorized Operation) when calling the DescribeInstanceStatus operation: You are not authorized to perform this operation. Please Refer to Automation Service Troubleshooting Guide for more diagnosis details.`
  - Correção: verifique se você forneceu o perfil de execução correto. Se isso foi feito, adicione a permissão necessária e execute novamente a avaliação.
- A execução foi bem-sucedida, mas não teve o resultado esperado. Isso é resultado de parâmetros incorretos ou de um problema de automação interna.
  - Mensagem de falha: a execução foi bem-sucedida, portanto, nenhuma mensagem de erro é exibida.
  - Remediação: verifique os parâmetros de entrada e observe as etapas executadas conforme explicado na execução do AWS FIS experimento Analisar antes de examinar as etapas individuais em busca de entradas e saídas esperadas.

AWS FIS falhas de experimentos ao testar pods do Kubernetes em execução em seus clusters do Amazon Elastic Kubernetes Service

A seguir estão as falhas comuns do Amazon Elastic Kubernetes Service (Amazon EKS) encontradas ao testar pods do Kubernetes em execução em seus clusters do Amazon EKS:

- Configuração incorreta das funções do IAM para AWS FIS experimentos ou para a conta de serviço do Kubernetes.
  - Mensagens de falha:
    - `Error resolving targets. Kubernetes API returned ApiException with error code 401.`
    - `Error resolving targets. Kubernetes API returned ApiException with error code 403.`
    - `Unable to inject AWS FIS Pod: Kubernetes API returned status code 403. Check Amazon EKS logs for more details.`
  - Correção: verifique o seguinte.

  - Certifique-se de ter seguido as instruções em Usar as ações do AWS FIS`aws:eks:pod`.
  - Certifique-se de ter criado e configurado uma conta de serviço do Kubernetes com as permissões RBAC necessárias e o namespace correto.
  - Certifique-se de ter mapeado a função do IAM fornecida (veja a saída da AWS CloudFormation pilha do teste) para o usuário do Kubernetes.
- Não foi possível iniciar o AWS FIS Pod: atingiu o máximo de contêineres secundários com falha. Isso geralmente acontece quando a memória não é suficiente para executar o AWS FIS contêiner auxiliar.
  - Mensagem de falha: `Unable to heartbeat FIS Pod: Max failed sidecar containers reached`.
  - Correção: uma opção para evitar esse erro é reduzir a porcentagem de carga desejada a ser alinhada com a memória ou a CPU disponíveis.
- A afirmação do alarme falhou no início do experimento. Esse erro ocorre porque o alarme relacionado não tem ponto de dados.
  - Mensagem de falha: `Assertion failed for the following alarms` Lista todos os alarmes para os quais a afirmação falhou.
  - Correção: certifique-se que o Container Insights esteja instalado corretamente para os alarmes e que o alarme não esteja ligado (no estado `ALARM`).

Entender as pontuações de resiliência

Esta seção descreve como AWS Resilience Hub quantifica a prontidão do aplicativo em diferentes cenários de interrupção.

AWS Resilience Hub fornece uma pontuação de resiliência que representa a postura de resiliência do aplicativo. Essa pontuação reflete o quanto o aplicativo segue nossas recomendações para atender à política de resiliência, aos alarmes, aos procedimentos operacionais padrão (SOPs) e aos testes do aplicativo. Com base no tipo de recursos que o aplicativo usa, AWS Resilience Hub recomenda alarmes e um conjunto de testes para cada tipo de interrupção. SOPs

A pontuação máxima de resiliência é de 100 pontos. Para obter a melhor pontuação possível ou a pontuação máxima, você deve implementar todos os alarmes e testes recomendados em seu aplicativo. SOPs Por exemplo, AWS Resilience Hub recomenda um teste com um alarme e umSOP. O teste é executado, dispara o alarme e inicia o associadoSOP. Se funcionar bem e se o aplicativo

atender à política de resiliência, ele receberá uma pontuação de resiliência próxima ou igual a 100 pontos.

Depois de executar a primeira avaliação, AWS Resilience Hub oferece a opção de excluir recomendações operacionais do seu aplicativo. Para entender o impacto das recomendações excluídas na pontuação de resiliência, você deve executar uma nova avaliação. No entanto, você sempre pode incluir as recomendações excluídas em sua inscrição e executar uma nova avaliação. Para obter mais informações sobre como incluir e excluir recomendações de alarmes e testes, consultethe section called “Incluir ou excluir recomendações operacionais”. SOP

Como acessar a pontuação de resiliência de seus aplicativos

Você pode visualizar a pontuação de resiliência do seu aplicativo escolhendo Painel ou Aplicativos no menu de navegação.

Acessar a pontuação de resiliência no painel

1. No menu de navegação esquerdo, escolha Painel.
2. Em Pontuação de resiliência do aplicativo ao longo do tempo, escolha um ou mais aplicativos na lista suspensa Escolha até 4 aplicativos.
3. O gráfico de Pontuação de resiliência exibe a pontuação de resiliência de todos os aplicativos escolhidos.

Acessar a pontuação de resiliência dos aplicativos

1. No menu de navegação esquerdo, escolha Aplicativos.
2. Em Aplicativos, abra um aplicativo.
3. Escolha Resumo.

   O gráfico de pontuação de resiliência exibe a tendência da pontuação de resiliência do seu aplicativo por até um ano. AWS Resilience Hub exibe itens de ação, violações da política de resiliência e recomendações operacionais que precisam ser abordadas para melhorar e alcançar a pontuação máxima de resiliência possível usando o seguinte:

   - Para visualizar os itens de ação que precisam ser realizados para melhorar e alcançar a pontuação máxima de resiliência possível, escolha a guia Itens de ação. Quando selecionado, AWS Resilience Hub exibe o seguinte:

- RTO/RPO— Indica o número de tempos de recuperação (RTO/RPOs) que precisam ser corrigidos para resolver as violações na política de resiliência do seu aplicativo. Escolha o valor para ver os RPO detalhesRTO/no relatório de avaliação do seu aplicativo.
- Alarmes — Indica o número de CloudWatch alarmes recomendados da Amazon que precisam ser implementados em seu aplicativo. Escolha o valor para visualizar os CloudWatch alarmes da Amazon que precisam ser corrigidos no relatório de avaliação do seu aplicativo.
- SOPs— Indica o número de recomendações SOPs que precisam ser implementadas em seu aplicativo. Escolha o valor para visualizar o SOPs que precisa ser corrigido no relatório de avaliação de sua inscrição.
- FIS— Indica o número de testes recomendados que precisam ser implementados em seu aplicativo. Escolha o valor para visualizar os testes que precisam ser corrigidos no relatório de avaliação do seu aplicativo.

- Para visualizar a pontuação de cada componente que afeta sua pontuação de resiliência, escolha Detalhamento da pontuação. Quando selecionado, o AWS Resilience Hub exibe o seguinte:
  - RTO/RPOconformidade — Indica a conformidade dos componentes de aplicativos (AppComponents) com os tempos estimados de recuperação da carga de trabalho e os tempos de recuperação desejados definidos na política de resiliência do seu aplicativo. Escolha o valor para visualizar as RPO estimativasRTO/no relatório de avaliação do seu aplicativo.
  - Alarmes implementados — Indica a contribuição real dos CloudWatch alarmes implementados da Amazon em comparação com sua contribuição máxima possível para a pontuação de resiliência do seu aplicativo. Escolha o valor para visualizar os CloudWatch alarmes implementados da Amazon no relatório de avaliação do seu aplicativo.
  - SOPsimplementado — Indica a contribuição real do implementado SOPs em comparação com sua contribuição máxima possível para a pontuação de resiliência do seu aplicativo. Escolha o valor para visualizar o implementado SOPs no relatório de avaliação do seu aplicativo.
  - FISexperimentos implementados — Indica a contribuição real dos testes implementados em comparação com sua contribuição máxima possível para a pontuação de resiliência do seu aplicativo. Escolha o valor para visualizar os testes implementados no relatório de avaliação do seu aplicativo.

- Para ver as violações da política de resiliência e as recomendações operacionais, escolha a seta direita para expandir a seção Violação da política e detalhamento das recomendações operacionais. Quando expandido, AWS Resilience Hub exibe o seguinte:
  - Violações da política de resiliência: indica o número de componentes do aplicativo que violam a política de resiliência do seu aplicativo. Escolha o valor ao lado de RTO/RPOpara ver os detalhes na guia Recomendações de resiliência do relatório de avaliação do seu aplicativo.
  - Recomendações operacionais: indica as recomendações operacionais que não foram implementadas ou executadas para melhorar a resiliência do seu aplicativo usando as guias Pendentes e Excluídos. As recomendações operacionais incluem todas as recomendações que estão inativas e as que não foram implementadas.

    Para ver as recomendações operacionais que precisam ser implementadas, escolha a guia Pendentes. Quando selecionado, AWS Resilience Hub exibe o seguinte:

    - Alarmes — Indica o número de CloudWatch alarmes recomendados da Amazon que precisam ser implementados.
    - SOPs— Indica o número de recomendações SOPs que precisam ser implementadas.
    - FIS— Indica o número de testes recomendados que precisam ser implementados.

    Para visualizar as recomendações operacionais que são excluídas do seu aplicativo, escolha a guia Excluídos. Quando selecionado, AWS Resilience Hub exibe o seguinte:

    - Alarmes — Indica o número de CloudWatch alarmes recomendados da Amazon que foram excluídos do seu aplicativo.
    - SOPs— Indica o número de recomendações SOPs que são excluídas do seu aplicativo.
    - FIS— Indica o número de testes recomendados que são excluídos da sua inscrição.

Como calcular as pontuações de resiliência

As tabelas desta seção explicam as fórmulas usadas AWS Resilience Hub para determinar os componentes de pontuação de cada tipo de recomendação e a pontuação de resiliência do seu aplicativo. Todos os valores resultantes determinados AWS Resilience Hub pelos componentes de pontuação de cada tipo de recomendação e pela pontuação de resiliência do seu aplicativo são arredondados para o ponto mais próximo. Por exemplo, se dois dos três alarmes forem implementados, a pontuação seria 13,33 ((2/3) * 20) pontos. Esse valor será arredondado para 13

pontos. Para obter mais informações sobre pesos usados nas fórmulas nas tabelas, consulte a seção the section called “Pesos AppComponents e tipos de interrupção”.

Alguns dos componentes de pontuação podem ser obtidos somente por meio do `ScoringComponentResiliencyScore`API. Para obter mais informações sobre issoAPI, consulte ScoringComponentResiliencyScore.

Tabelas

- Fórmulas para calcular o componente de pontuação de cada tipo de recomendação
- Fórmula para calcular a pontuação de resiliência
- Fórmulas para calcular a pontuação de resiliência AppComponents e os tipos de interrupção

A tabela a seguir explica as fórmulas usadas AWS Resilience Hub para calcular o componente de pontuação de cada tipo de recomendação.

Fórmulas para calcular o componente de pontuação de cada tipo de recomendação

Componente de pontuação	Descrição	Fórmula	Exemplo
Cobertura do teste (T)	Uma pontuação normalizada (0 a 100 pontos) com base no número de testes que foram implementados e excluídos com sucesso, do número total de testes do AWS Resilience Hub recomendados. **Note** Para calcular a pontuação de resiliência, os testes recomendados devem ter sido executados	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)` As partes da fórmula são as seguintes: • Número total de testes configurados — Indica o número total de testes configurados quando o AWS CloudFormation modelo é criado e carregado no AWS	Se você implementou 10 e excluiu 5 dos 20 testes do AWS Resilience Hub recomendados, a cobertura do teste é calculada da seguinte forma: `T = (10 + 5) / 20` Ou seja, `T = .75 or 75 points`

Componente de pontuação	Descrição	Fórmula	Exemplo
	com sucesso nos últimos 30 dias AWS Resilience Hub para considerá-la como implementada.	CloudFormation console. • Número total de testes recomendados — Indica os testes recomendados por AWS Resilience Hub com base nos recursos do aplicativo. • Número total de testes excluídos: indica o número de testes recomendados que você excluiu do aplicativo.	

Componente de pontuação	Descrição	Fórmula	Exemplo
Cobertura de alarmes (A)	Uma pontuação normalizada (0 a 100 pontos) com base no número de CloudWatch alarmes da Amazon que foram implementados e excluídos com sucesso, do número total de alarmes recomendados pela AWS Resilience Hub Amazon. CloudWatch **Note** Para calcular a pontuação de resiliência, os alarmes recomendados devem estar no estado Pronto para que o AWS Resilience Hub os considere como implementados.	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` As partes da fórmula são as seguintes: • Número total de alarmes configurados — Indica o número total de CloudWatch alarmes da Amazon configurados quando o AWS CloudFormation modelo é criado e carregado no AWS CloudFormation console. • Número total de alarmes recomendados — Indica os CloudWatch alarmes recomendados pela Amazon AWS Resilience Hub com base nos recursos do aplicativo. • Número total de alarmes excluídos — Indica o número de CloudWatch alarmes recomendados	Se você implementou 10 e excluiu 5 alarmes da Amazon dos 20 CloudWatch alarmes AWS Resilience Hub recomendados da Amazon, a cobertura de CloudWatch alarmes da Amazon CloudWatch é calculada da seguinte forma: `A = (10 + 5) / 20` Ou seja, `A = .75 or 75 points`

Componente de pontuação	Descrição	Fórmula	Exemplo
		da Amazon que você excluiu do aplicativo.	

Componente de pontuação	Descrição	Fórmula	Exemplo
SOPcobertura (S)	Uma pontuação normalizada (0 a 100 pontos) com base no número dos SOPs que foram implementados e excluídos com sucesso, do número total de AWS Resilience Hub recomendados. SOPs	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` As partes da fórmula são as seguintes: • Número total de SOPs configurados — Indica o número total de SOPs configurados quando o AWS CloudFormation modelo é criado e carregado no AWS CloudFormation console. • Número total de SOPs recomendados — Indica o SOPs recomendado por AWS Resilience Hub com base nos recursos do aplicativo. • Número total de SOPs excluídos — Indica o número de itens recomendados que SOPs você excluiu do aplicativo.	Se você implementou 10 e excluiu 5 SOPs das 20 AWS Resilience Hub recomendadasSOPs, a SOP cobertura é calculada da seguinte forma: `S = (10 + 5) / 20` Ou seja, `S = .75 or 75 points`

Componente de pontuação	Descrição	Fórmula	Exemplo
RTO/RPOconformidade (P)	Uma pontuação normalizada (0 a 100 pontos) com base no cumprimento da política de resiliência do aplicativo.	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	Se sua política de resiliência de aplicativos atender somente aos tipos de zona de disponibilidade (AZ) e de interrupção da infraestrutura, a pontuação da política de resiliência (P) será calculada da seguinte forma: • Se você definiu RPO metas regionais RTO e regionais, P é calculado da seguinte forma: `P = (20 + 30)/ 100` Ou seja, `P = .5 or 50 points` • Se você não definiu RPO metas RTO e regiões, P é calculado da seguinte forma:

Componente de pontuação	Descrição	Fórmula	Exemplo
			`P = (22.22 + 33.33)/ 99.9` Ou seja, `P = .55 or 55 points`

A tabela a seguir explica a fórmula usada AWS Resilience Hub para calcular a pontuação de resiliência de todo o aplicativo.

Fórmula para calcular a pontuação de resiliência

Componente de pontuação	Descrição	Fórmula	Exemplo

Pontuação de resiliência do aplicativo (`RS`)	Uma pontuação de resiliência normalizada (0 a 100 pontos) com base no cumprimento da política de resiliência pelo aplicativo. A pontuação de resiliênc ia por aplicativo é a média ponderada de todos os tipos de recomendação. Ou seja: `RS = Weighted Average (T, A, S, P)`	A pontuação de resiliência por aplicativo é calculada usando a seguinte fórmula: `RS = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			As fórmulas para calcular a cobertura de cada tabela de tipo de recomendação são as seguintes:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`

Componente de pontuação	Descrição	Fórmula	Exemplo
			A pontuação de resiliência por aplicativo é calculada da seguinte forma: `RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4)` Ou seja, `RS = .65 or 65 points`

A tabela a seguir explica as fórmulas usadas AWS Resilience Hub para calcular a pontuação de resiliência dos componentes do aplicativo (AppComponents) e dos tipos de interrupção. No entanto, você pode obter a pontuação de resiliência AppComponents e os tipos de interrupção somente por meio do seguinte AWS Resilience Hub: APIs

- DescribeAppAssessmentpara obter `RSo`
- ListAppComponentCompliancespara obter `RSao` e `RSA`

Fórmulas para calcular a pontuação de resiliência AppComponents e os tipos de interrupção

Componente de pontuação	Descrição	Fórmula	Exemplo
Pontuação de resiliência por AppCompon ent e por tipo	Uma pontuação normalizada (0 a 100 pontos)	A pontuação de resiliência por tipo de interrupção AppComponent e por tipo de interrupção é calculada usando a seguinte fórmula:	As suposições de `RSao` para todos os tipos de recomenda ção são as seguintes:

Componente de pontuação	Descrição	Fórmula	Exemplo

de interrupção () `RSao`	com base no AppComponent cumprimento de sua política de resiliência por tipo de interrupção. A pontuação de resiliência por AppComponent tipo de interrupção é a média ponderada de todos os tipos de recomendação.
	
	Ou seja: `RSao = Weighted Average (T, A, S, P)`
	
	Os valores de `T, A, S, P` são calculados para todos os testes e alarmes recomendados e para atender à política de resiliênc
		`RSao = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			A pontuação de resiliência por tipo AppComponent de interrupção é calculada da seguinte forma:
			
			`RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)`
			
			Ou seja, `RSao = .65 or 65 points`

Componente de pontuação	Descrição	Fórmula	Exemplo
	ia do tipo AppComponent e do tipo de interrupção. SOPs		

Componente de pontuação	Descrição	Fórmula	Exemplo
Pontuação de resiliência por AppComponent () RSa	Uma pontuação normalizada (0 a 100 pontos) com base no cumprimento de sua política de resiliência. A pontuação de resiliência per AppComponent é a média ponderada de todos os tipos de recomendação. Ou seja: RSa = Weighted Average (T, A, S, P) Os valores de T, A, S, P são calculados para todos os testes e alarmes recomendados e para atender à política de resiliência do. SOPs	A pontuação de resiliência per AppComponent é calculada usando a seguinte fórmula: RSa = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	As suposições de RSa para todos os tipos de recomendação são as seguintes: • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 A pontuação de resiliência por AppComponent é calculada da seguinte forma: RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) Ou seja, RSa = .65 or 65 points

Componente de pontuação	Descrição	Fórmula	Exemplo
	AppComponent		

Componente de pontuação	Descrição	Fórmula	Exemplo

Pontuação de resiliência por tipo de interrupção (RSo)	Uma pontuação normalizada (0 a 100 pontos) com base no cumprimento de sua política de resiliência. A pontuação de resiliência por tipo de interrupção é a média ponderada de todos os tipos de recomendação. Ou seja: `RSo = Weighted Average (T, A, S, P)`
	
	Os valores de `T, A, S, P` são calculados para todos os testes e alarmes recomendados e para atender à política de resiliência do tipo de
		A pontuação de resiliência por tipo de interrupção é calculada usando a seguinte fórmula:
		
		`RSo = (T * Weight(T) + A * Weight(A) +`
		
		`S * Weight(S) + P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			As suposições de `RSo` para todos os tipos de recomendação são as seguintes:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			A pontuação de resiliência por tipo de interrupção é calculada da seguinte forma:
			
			`RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) /`
			
			`(.2 + .2 + .2 + .4)`
			
			Ou seja, `RSo = .65 or 65 points`

Componente de pontuação	Descrição	Fórmula	Exemplo
	interrupção. SOPs		

Pesos

AWS Resilience Hub atribui um peso a cada tipo de recomendação para a pontuação total de resiliência.

As tabelas a seguir mostram o peso dos alarmes, testesSOPs, da política de resiliência de reuniões e dos tipos de interrupção. Os tipos de interrupções incluem aplicativo, infraestrutura, AZ e Região.

> **Note**
>
> Se você optar por não definir regiões RTO ou RPO metas para sua política, os pesos dos outros tipos de interrupção serão aumentados de acordo, conforme mostrado na coluna Peso quando a região não está definida.

Pesos para alarmesSOPs, testes e metas políticas

Tipo de recomendação	Weight
Alarmes	20 pontos
SOPs	20 pontos
Testes	20 pontos
Cumpre a política de resiliência	40 pontos

Pesos para o tipo de interrupção

Tipo de interrupção	Peso quando a região é definida	Peso quando a região não é definida
Aplicativo	40 pontos	44,44 pontos

Tipo de interrupção	Peso quando a região é definida	Peso quando a região não é definida
Infraestrutura	30 pontos	33,33 pontos
Zona de disponibilidade	20 pontos	22,22 pontos
Região	10 pontos	N/D

Integrando recomendações operacionais em seu aplicativo com AWS CloudFormation

Depois de escolher Criar CloudFormation modelo na página de recomendações operacionais, AWS Resilience Hub cria um AWS CloudFormation modelo que descreve o alarme específico, o procedimento operacional padrão (SOP) ou o AWS FIS experimento para seu aplicativo. O AWS CloudFormation modelo é armazenado em um bucket do Amazon S3, e você pode verificar o caminho do S3 até o modelo na guia Detalhes do modelo na página de recomendações operacionais.

Por exemplo, a lista abaixo mostra um AWS CloudFormation modelo JSON formatado que descreve uma recomendação de alarme renderizada por. AWS Resilience HubÉ um alarme Read Throttling (Controle de utilização de Leitura) para uma tabela do DynamoDB chamada `Employees`.

A seção `Resources` do modelo descreve o alarme do `AWS::CloudWatch::Alarm` que é ativado quando o número de eventos de controle de utilização de leitura da tabela do DynamoDB excede 1. E os dois `AWS::SSM::Parameter` recursos definem metadados que permitem AWS Resilience Hub identificar os recursos instalados sem precisar escanear o aplicativo real.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the Amazon SNS topic to which alarm status changes
 are to be sent. This must be in the same Region being deployed.",
      "AllowedPattern" : "^arn:(aws|aws-cn|aws-iso|aws-iso-[a-z]{1}|aws-us-gov):sns:
([a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-[0-9]):[0-9]{12}:[A-Za-z0-9/][A-Za-
z0-9:_/+=,@.-]{1,256}$"
    }
```

```
  },
  "Resources" : {

 "ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm" :
 {
      "Type" : "AWS::CloudWatch::Alarm",
      "Properties" : {
        "AlarmDescription" : "An Alarm by AWS Resilience Hub that alerts when the
 number of read-throttle events are greater than 1.",
        "AlarmName" : "ResilienceHub-ReadThrottleEventsAlarm-2020-04-01_Employees-ON-
DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9",
        "AlarmActions" : [ {
          "Ref" : "SNSTopicARN"
        } ],
        "MetricName" : "ReadThrottleEvents",
        "Namespace" : "AWS/DynamoDB",
        "Statistic" : "Sum",
        "Dimensions" : [ {
          "Name" : "TableName",
          "Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
        } ],
        "Period" : 60,
        "EvaluationPeriods" : 1,
        "DatapointsToAlarm" : 1,
        "Threshold" : 1,
        "ComparisonOperator" : "GreaterThanOrEqualToThreshold",
        "TreatMissingData" : "notBreaching",
        "Unit" : "Count"
      },
      "Metadata" : {
        "AWS::ResilienceHub::Monitoring" : {
          "recommendationId" : "dynamodb:alarm:health-read_throttle_events:2020-04-01"
        }
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
        "Name" : "/ResilienceHub/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/dynamodb-
alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-DynamoDBTable-
PXBZQYH3DCJ9",
        "Type" : "String",
```

```
        "Value" : {
          "Fn::Sub" :
 "${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
        "Name" : "/ResilienceHub/Info/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/
dynamodb-alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-
DynamoDBTable-PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    }
  }
}
```

Modificando o modelo AWS CloudFormation

A maneira mais fácil de integrar um alarme ou AWS FIS recurso em seu aplicativo principal é simplesmente adicioná-lo como outro recurso no modelo que descreve seu modelo de aplicativo. SOP O arquivo JSON formatado abaixo fornece uma descrição básica de como uma tabela do DynamoDB é descrita em um modelo. AWS CloudFormation É provável que um aplicativo real inclua vários outros recursos, como tabelas adicionais.

```
{
   "AWSTemplateFormatVersion": "2010-09-09T00:00:00.000Z",
   "Description": "Application Stack with Employees Table",
   "Outputs": {
      "DynamoDBTable": {
```

```
            "Description": "The DynamoDB Table Name",
            "Value": {"Ref": "Employees"}
        }
    },
    "Resources": {
        "Employees": {
            "Type": "AWS::DynamoDB::Table",
            "Properties": {
                "BillingMode": "PAY_PER_REQUEST",
                "AttributeDefinitions": [
                    {
                        "AttributeName": "USER_ID",
                        "AttributeType": "S"
                    },
                    {
                        "AttributeName": "RANGE_ATTRIBUTE",
                        "AttributeType": "S"
                    }
                ],
                "KeySchema": [
                    {
                        "AttributeName": "USER_ID",
                        "KeyType": "HASH"
                    },
                    {
                        "AttributeName": "RANGE_ATTRIBUTE",
                        "KeyType": "RANGE"
                    }
                ],
                "PointInTimeRecoverySpecification": {
                    "PointInTimeRecoveryEnabled": true
                },
                "Tags": [
                    {
                        "Key": "Key",
                        "Value": "Value"
                    }
                ],
                "LocalSecondaryIndexes": [
                    {
                        "IndexName": "resiliencehub-index-local-1",
                        "KeySchema": [
                            {
                                "AttributeName": "USER_ID",
```

```
                        "KeyType": "HASH"
                     },
                     {
                        "AttributeName": "RANGE_ATTRIBUTE",
                        "KeyType": "RANGE"
                     }
                  ],
                  "Projection": {
                     "ProjectionType": "ALL"
                  }
               }
            ],
            "GlobalSecondaryIndexes": [
               {
                  "IndexName": "resiliencehub-index-1",
                  "KeySchema": [
                     {
                        "AttributeName": "USER_ID",
                        "KeyType": "HASH"
                     }
                  ],
                  "Projection": {
                     "ProjectionType": "ALL"
                  }
               }
            ]
         }
      }
   }
}
```

Para permitir que o recurso de alarme seja implantado com seu aplicativo, agora você precisa substituir os recursos codificados por uma referência dinâmica nas pilhas de aplicativos.

Então, na definição do recurso do `AWS::CloudWatch::Alarm`, altere o seguinte:

```
"Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
```

para aquele abaixo:

```
"Value" : {"Ref": "Employees"}
```

E, na definição do recurso do `AWS::SSM::Parameter`, altere o seguinte:

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededDynamoDBEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

para aquele abaixo:

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",\"resourceId
\":\"${Employees}\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

Ao modificar AWS CloudFormation modelos SOPs e AWS FIS experimentos, você adotará a mesma abordagem, substituindo a referência IDs codificada por referências dinâmicas que continuam funcionando mesmo após alterações de hardware.

Ao usar uma referência à tabela do DynamoDB, você AWS CloudFormation permite fazer o seguinte:

- Crie primeiro a tabela do banco de dados.
- Sempre use a ID real do recurso gerado no alarme e atualize o alarme dinamicamente se AWS CloudFormation precisar substituir o recurso.

> **Note**
>
> Você pode escolher métodos mais avançados para gerenciar os recursos do seu aplicativo AWS CloudFormation , como pilhas de aninhamento ou consultar saídas de recursos em uma pilha separada. AWS CloudFormation (Porém, se você quiser manter a pilha de recomendações separada da pilha principal, precisará configurar uma forma de transmitir informações entre as duas pilhas).
> Além disso, ferramentas de terceiros, como o Terraform by HashiCorp, também podem ser usadas para provisionar Infraestrutura como Código (IaC).

Usando AWS Resilience Hub APIs para descrever e gerenciar o aplicativo

Como alternativa para descrever e gerenciar aplicativos usando o AWS Resilience Hub console, AWS Resilience Hub permite que você descreva e gerencie aplicativos usando AWS Resilience Hub APIs. Este capítulo explica como criar um aplicativo usando AWS Resilience Hub APIs o. Ele também define a sequência na qual você precisa executar APIs e os valores dos parâmetros que você deve fornecer com exemplos apropriados. Para obter mais informações, consulte os tópicos a seguir.

- the section called “Preparar o aplicativo”
- the section called “Executar e analisar o aplicativo”
- the section called “Modificar seu aplicativo”

Etapa 1: preparar o aplicativo

Para preparar um aplicativo, você deve primeiro criar um aplicativo, atribuir uma política de resiliência e, em seguida, importar os recursos do aplicativo de suas fontes de entrada. Para obter mais informações sobre os AWS Resilience Hub APIs que são usados para preparar um aplicativo, consulte os tópicos a seguir:

- the section called “Criar um aplicativo”
- the section called “Criar política de resiliência”
- the section called “Importar recurso do aplicativo e monitorar status da importação”
- the section called “Publicar seu aplicativo e atribuir uma política de resiliência”

Criar um aplicativo

Para criar um novo aplicativo em AWS Resilience Hub, você deve chamar o `CreateApp` API e fornecer um nome de aplicativo exclusivo. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

O exemplo a seguir mostra como criar um novo aplicativo `newApp` AWS Resilience Hub usando `CreateApp`API.

Solicitação

```
aws resiliencehub create-app --name newApp
```

Resposta

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {},
        "assessmentSchedule": "Disabled"
    }
}
```

Criar política de resiliência

Depois de criar o aplicativo, você deve criar uma política de resiliência que permita entender a postura de resiliência do seu aplicativo usando. `CreateResiliencyPolicy` API Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html.

O exemplo a seguir mostra como criar `newPolicy` para seu aplicativo AWS Resilience Hub usando `CreateResiliencyPolicy`API.

Solicitação

```
aws resiliencehub create-resiliency-policy \
--policy-name newPolicy --tier NonCritical \
--policy '{"AZ": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Hardware": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Software": {"rtoInSecs": 172800,"rpoInSecs": 86400}}'
```

Resposta

```
{
```

```
    "policy": {
        "policyArn": "<Policy_ARN>",
        "policyName": "newPolicy",
        "policyDescription": "",
        "dataLocationConstraint": "AnyLocation",
        "tier": "NonCritical",
        "estimatedCostTier": "L1",
        "policy": {
            "AZ": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Hardware": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Software": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            }
        },
        "creationTime": "2022-10-26T20:48:05.946000+03:00",
        "tags": {}
    }
}
```

Importar recursos de uma fonte de entrada e monitorar o status da importação

AWS Resilience Hub fornece o seguinte APIs para importar recursos para seu aplicativo:

- `ImportResourcesToDraftAppVersion`— Isso API permite que você importe recursos para a versão de rascunho do seu aplicativo a partir de diferentes fontes de entrada. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- `PublishAppVersion`— Isso API publica uma nova versão do aplicativo junto com a atualizada AppComponents. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.
- `DescribeDraftAppVersionResourcesImportStatus`— Isso API permite monitorar o status de importação de seus recursos para uma versão do aplicativo. Para obter mais informações

sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

O exemplo a seguir mostra como importar recursos para seu aplicativo AWS Resilience Hub usando `ImportResourcesToDraftAppVersion`API.

Solicitação

```
aws resiliencehub import-resources-to-draft-app-version \
--app-arn <App_ARN> \
--terraform-sources '[{"s3StateFileUrl": <S3_URI>}]'
```

Resposta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "sourceArns": [],
    "status": "Pending",
    "terraformSources": [
        {
            "s3StateFileUrl": <S3_URI>
        }
    ]
}
```

O exemplo a seguir mostra como adicionar recursos manualmente ao seu aplicativo AWS Resilience Hub usando `CreateAppVersionResource`API.

Solicitação

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

Resposta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

O exemplo a seguir mostra como monitorar o status de importação de seus recursos em AWS Resilience Hub uso `DescribeDraftAppVersionResourcesImportStatus`API.

Solicitação

```
aws resiliencehub describe-draft-app-version-resources-import-status \
--app-arn <App_ARN>
```

Resposta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "status": "Success",
    "statusChangeTime": "2022-10-26T19:55:18.471000+03:00"
}
```

Publicar a versão preliminar do seu aplicativo e atribuir uma política de resiliência

Antes de executar uma avaliação, você deve primeiro publicar a versão preliminar do seu aplicativo e atribuir uma política de resiliência à versão lançada do seu aplicativo.

Publicar a versão preliminar do seu aplicativo e atribuir uma política de resiliência

1. Para publicar a versão de rascunho do seu aplicativo, use `PublishAppVersion`API. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

   O exemplo a seguir mostra como publicar a versão de rascunho do aplicativo AWS Resilience Hub usando `PublishAppVersion`API.

   Solicitação

   ```
   aws resiliencehub publish-app-version \
    --app-arn <App_ARN>
   ```

   Resposta

   ```
   {
       "appArn": "<App_ARN>",
       "appVersion": "release"
   }
   ```

2. Aplique uma política de resiliência à versão lançada do seu aplicativo usando `UpdateApp`API. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html.

   O exemplo a seguir mostra como aplicar uma política de resiliência à versão lançada de um aplicativo em AWS Resilience Hub uso `UpdateApp`API.

   Solicitação

   ```
   aws resiliencehub update-app \
   ```

```
--app-arn <App_ARN> \
--policy-arn <Policy_ARN>
```

Resposta

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "policyArn": "<Policy_ARN>",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {
            "resourceArn": "<App_ARN>"
        },
        "assessmentSchedule": "Disabled"
    }
}
```

Etapa 2: executar e gerenciar avaliações de resiliência do AWS Resilience Hub

Depois de publicar uma nova versão do seu aplicativo, você deve executar uma nova avaliação de resiliência e analisar os resultados para garantir que seu aplicativo atenda à carga de trabalho estimada RTO e estimada RPO que estão definidas em sua política de resiliência. A avaliação compara a configuração de cada componente do aplicativo com a política e faz recomendações de SOP alarmes e testes.

Para obter mais informações, consulte os tópicos a seguir.

- the section called “Executar e monitorar uma avaliação de resiliência”
- the section called “Criar política de resiliência”

Executar e monitorar avaliações de resiliência do AWS Resilience Hub

Para executar avaliações de resiliência AWS Resilience Hub e monitorar seu status, você deve usar o seguinte: APIs

- `StartAppAssessment`— Isso API cria uma nova avaliação para um aplicativo. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.
- `DescribeAppAssessment`— Isso API descreve uma avaliação para a inscrição e fornece o status de conclusão da avaliação. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

O exemplo a seguir mostra como começar a executar uma nova avaliação no AWS Resilience Hub uso `StartAppAssessment`API.

Solicitação

```
aws resiliencehub start-app-assessment \
--app-arn <App_ARN> \
--app-version release \
--assessment-name first-assessment
```

Resposta

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "invoker": "User",
        "assessmentStatus": "Pending",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
```

```
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

O exemplo a seguir mostra como monitorar o status de sua avaliação no AWS Resilience Hub uso `DescribeAppAssessment`API. Você pode extrair o status da sua avaliação da variável `assessmentStatus`.

Solicitação

```
aws resiliencehub describe-app-assessment \
--assessment-arn <Assessment_ARN>
```

Resposta

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "cost": {
            "amount": 0.0,
            "currency": "USD",
            "frequency": "Monthly"
        },
        "resiliencyScore": {
            "score": 0.27,
            "disruptionScore": {
                "AZ": 0.42,
                "Hardware": 0.0,
                "Region": 0.0,
```

```
                "Software": 0.38
            }
        },
        "compliance": {
            "AZ": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            },
            "Hardware": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 2595601,
                "currentRpoInSecs": 2592001,
                "complianceStatus": "PolicyBreached",
                "achievableRpoInSecs": 0
            },
            "Software": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            }
        },
        "complianceStatus": "PolicyBreached",
        "assessmentStatus": "Success",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "endTime": "2022-10-27T08:15:31.883000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
```

```
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

Examinar resultados da avaliação

Depois que sua avaliação for concluída com sucesso, você poderá examinar os resultados da avaliação usando o seguinteAPIs.

- `DescribeAppAssessment`— Isso API permite que você acompanhe o status atual do seu aplicativo em relação à política de resiliência. Além disso, você também pode extrair o status de conformidade da variável `complianceStatus` e a pontuação de resiliência para cada tipo de interrupção da estrutura `resiliencyScore`. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.
- `ListAlarmRecommendations`— Isso API permite que você obtenha as recomendações de alarme usando o Amazon Resource Name (ARN) da avaliação. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html.

> **Note**
>
> Para obter as recomendações SOP e FIS testar, use `ListSopRecommendations` `ListTestRecommendations` APIs e.

O exemplo a seguir mostra como obter as recomendações de alarme usando o Amazon Resource Name (ARN) da avaliação usando `ListAlarmRecommendations`API.

> **Note**
>
> Para obter as recomendações SOP e FIS testar, substitua por `ListSopRecommendations` ou`ListTestRecommendations`.

Solicitação

```
aws resiliencehub list-alarm-recommendations \
--assessment-arn <Assessment_ARN>
```

Resposta

```
{
    "alarmRecommendations": [
        {
            "recommendationId": "78ece7f8-c776-499e-baa8-b35f5e8b8ba2",
            "referenceId": "app_common:alarm:synthetic_canary:2021-04-01",
            "name": "AWSResilienceHub-SyntheticCanaryInRegionAlarm_2021-04-01",
            "description": "A monitor for the entire application, configured to
 constantly verify that the application API/endpoints are available",
            "type": "Metric",
            "appComponentName": "appcommon",
            "items": [
                {
                    "resourceId": "us-west-2",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure Amazon CloudWatch Synthetics is setup to monitor
 the application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/
latest/monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>).
 \nMake sure that the Synthetics Name passed in the alarm dimension matches the name of
 the Synthetic Canary. It Defaults to the name of the application.\n"
        },
        {
            "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
            "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
            "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
```

```
            "description": "An alarm by AWS Resilience Hub that reports when Amazon EFS
 I/O load is more than 90% for too much time",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "09f340cd-3427-4f66-8923-7f289d4a3216",
            "referenceId": "efs:alarm:mount_failure:2020-04-01",
            "name": "AWSResilienceHub-EFSMountFailureAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when volume
 failed to mount to EC2 instance",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "* Make sure Amazon EFS utils are installed(see the <a
 href=\"https://github.com/aws/efs-utils#installation\" target=\"_blank\">docs</a>).
\n* Make sure cloudwatch logs are enabled in efs-utils (see the <a href=\"https://
github.com/aws/efs-utils#step-2-enable-cloudwatch-log-feature-in-efs-utils-config-
file-etcamazonefsefs-utilsconf\" target=\"_blank\">docs</a>).\n* Make sure that
 you've configured `log_group_name` in `/etc/amazon/efs/efs-utils.conf`, for example:
 `log_group_name = /aws/efs/utils`.\n* Use the created `log_group_name` in the
 generated alarm. Find `LogGroupName: REPLACE_ME` in the alarm and make sure the
 `log_group_name` is used instead of REPLACE_ME.\n"
        },
        {
            "recommendationId": "b0f57d2a-1220-4f40-a585-6dab1e79cee2",
            "referenceId": "efs:alarm:client_connections:2020-04-01",
            "name": "AWSResilienceHub-EFSHighClientConnectionsAlarm_2020-04-01",
```

```
            "description": "An alarm by AWS Resilience Hub that reports when client
 connection number deviation is over the specified threshold",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
            "referenceId": "rds:alarm:health-storage:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
            "description": "Reports when database free storage is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
            "referenceId": "rds:alarm:health-connections:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
            "description": "Reports when database connection count is anomalous",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
```

```
        },
        {
            "recommendationId": "f169b8d4-45c1-4238-95d1-ecdd8d5153fe",
            "referenceId": "rds:alarm:health-cpu:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceOverUtilizedCpuAlarm_2020-04-01",
            "description": "Reports when database used CPU is high",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "69da8459-cbe4-4ba1-a476-80c7ebf096f0",
            "referenceId": "rds:alarm:health-memory:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowMemoryAlarm_2020-04-01",
            "description": "Reports when database free memory is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "67e7902a-f658-439e-916b-251a57b97c8a",
            "referenceId": "ecs:alarm:health-service_cpu_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighCpuUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that triggers when CPU
 utilization of ECS tasks of Service exceeds the threshold",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
```

```
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "fb30cb91-1f09-4abd-bd2e-9e8ee8550eb0",
            "referenceId": "ecs:alarm:health-service_memory_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighMemoryUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that
 indicates if the percentage of memory that is used in the service, is exceeding
 specified threshold limit",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "1bd45a8e-dd58-4a8e-a628-bdbee234efed",
            "referenceId": "ecs:alarm:health-service_sample_count:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceSampleCountAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that triggers
 if the count of tasks isn't equal Service Desired Count",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure the Container Insights on Amazon ECS is enabled:
 (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/
deploy-container-insights-ECS-cluster.html\" target=\"_blank\">docs</a>)."
        }
```

```
    ]
}
```

O exemplo a seguir mostra como obter as recomendações de configuração (recomendações sobre como melhorar sua resiliência atual) usando `ListAppComponentRecommendations`API.

Solicitação

```
aws resiliencehub list-app-component-recommendations \
--assessment-arn <Assessment_ARN>
```

Resposta

```
{
    "componentRecommendations": [
        {
            "appComponentName": "computeappcomponent-nrz",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
 cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
 backups"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
 cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
```

```
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
```

```
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 14.74,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 in multiple AZs and CapacityProviders with
MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 and CapacityProviders with MinSize > 1",
                            "expectedRpoInSecs": 0,
```

```
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Stateful Amazon ECS service with launch type Amazon
EC2 and Amazon EFS storage, deployed in multiple AZs. AWS Backup is used to backup
Amazon EFS and copy snapshots in-Region.",
                    "suggestedChanges": [
                        "Add AWS Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove Amazon EBS volume"
                    ],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "ecs:config:ec2-multi_az-efs-backups:2022-02-16"
                }
            ]
        },
        {
            "appComponentName": "databaseappcomponent-hji",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
```

```
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
```

```
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 76.73,
```

```
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
                            "expectedRpoInSecs": 300,
                            "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
                    "suggestedChanges": [
                        "Add read replica in the same Region",
                        "Change DB instance to a supported class (db.t3.small)",
                        "Change to Aurora",
                        "Enable cluster backtracking",
                        "Enable instance backup with retention period 7"
                    ],
                    "haArchitecture": "WarmStandby",
```

```
                    "referenceId": "rds:config:aurora-backtracking"
                }
            ]
        },
        {
            "appComponentName": "storageappcomponent-rlb",
            "recommendationStatus": "BreachedUnattainable",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
```

```
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAttainable",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                }
```

```
            ]
        }
    ]
}
```

Etapa 3: modificar seu aplicativo

AWS Resilience Hub permite que você modifique os recursos do seu aplicativo editando uma versão de rascunho do seu aplicativo e publicando as alterações em uma nova versão (publicada). AWS Resilience Hub usa a versão publicada do seu aplicativo, que inclui os recursos atualizados, para executar avaliações de resiliência.

Para obter mais informações, consulte os tópicos a seguir.

- the section called “Adicionar recursos manualmente”
- the section called “Agrupar recursos em um único componente de aplicativo”
- the section called “Excluindo um recurso de um AppComponent”

Adicionar recursos manualmente ao seu aplicativo

Se o recurso não for implantado como parte de uma fonte de entrada, AWS Resilience Hub permite que você adicione manualmente o recurso ao seu aplicativo usando `CreateAppVersionResource`API. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

Você deve fornecer os seguintes parâmetros para issoAPI:

- Nome do recurso Amazon (ARN) do aplicativo
- ID lógico do recurso
- ID físico do recurso
- AWS CloudFormation digitar

O exemplo a seguir mostra como adicionar recursos manualmente ao seu aplicativo AWS Resilience Hub usando `CreateAppVersionResource`API.

Solicitação

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

Resposta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

Agrupar recursos em um único componente de aplicativo

Um componente de aplicativo (AppComponent) é um grupo de AWS recursos relacionados que funcionam e falham como uma única unidade. Por exemplo, quando você tem cargas de trabalho entre regiões que são usadas como implantações em espera. AWS Resilience Hub tem regras que regem quais AWS recursos podem pertencer a qual tipo de AppComponent. AWS Resilience

Hub permite agrupar recursos em um único AppComponent usando o seguinte gerenciamento de recursosAPIs.

- `UpdateAppVersionResource`— Isso API atualiza os detalhes do recurso de um aplicativo. Para obter mais informações sobre issoAPI, consulte UpdateAppVersionResource.
- `DeleteAppVersionAppComponent`— Isso API exclui o AppComponent do aplicativo. Para obter mais informações sobre issoAPI, consulte DeleteAppVersionAppComponent.

O exemplo a seguir mostra como atualizar os detalhes do recurso do seu aplicativo AWS Resilience Hub usando `DeleteAppVersionAppComponent`API.

Solicitação

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

Resposta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

O exemplo a seguir mostra como excluir o vazio AppComponent que foi criado nos exemplos anteriores em AWS Resilience Hub usando `UpdateAppVersionResource`API.

Solicitação

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

Resposta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

Excluindo um recurso de um AppComponent

AWS Resilience Hub permite que você exclua recursos das avaliações usando `UpdateAppVersionResource`API. Esses recursos não serão considerados ao calcular a resiliência do seu aplicativo. Para obter mais informações sobre issoAPI, consultehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html.

> **Note**
>
> Você pode excluir somente os recursos que foram importados de uma fonte de entrada.

O exemplo a seguir mostra como excluir um recurso do seu aplicativo no AWS Resilience Hub uso `UpdateAppVersionResource`API.

Solicitação

```
aws resiliencehub update-app-version-resource \
--app-arn <App_ARN> \
--resource-name "ec2instance-nvz" \
--excluded
```

Resposta

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
```

```
        "resourceName": "ec2instance-nvz",
        "logicalResourceId": {
            "identifier": "ec2",
            "terraformSourceName": "test.state.file"
        },
        "physicalResourceId": {
            "identifier": "i-0b58265a694e5ffc1",
            "type": "Native",
            "awsRegion": "us-west-2",
            "awsAccountId": "123456789101"
        },
        "resourceType": "AWS::EC2::Instance",
        "appComponents": [
            {
                "name": "computeappcomponent-nrz",
                "type": "AWS::ResilienceHub::ComputeAppComponent"
            }
        ]
    }
}
```

Segurança em AWS Resilience Hub

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 na AWS nuvem. 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 aplicáveis AWS Resilience Hub, consulte AWS Serviços no escopo do programa de conformidade 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 AWS Resilience Hub. Os tópicos a seguir mostram como configurar para atender AWS Resilience Hub aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Resilience Hub recursos.

Conteúdo

Proteção de dados em AWS Resilience Hub

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Resilience Hub. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle

sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

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 a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Resilience Hub ou outro Serviços da AWS usando o console,API, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Criptografia em repouso

AWS Resilience Hub criptografa seus dados em repouso. Os dados inseridos AWS Resilience Hub são criptografados em repouso usando criptografia transparente do lado do servidor. Isso ajuda

a reduzir a carga e a complexidade operacionais necessárias para proteger dados confidenciais. Com a criptografia de dados em repouso, você pode criar aplicativos confidenciais que atendem a requisitos de conformidade e regulamentação de criptografia.

Criptografia em trânsito

AWS Resilience Hub criptografa os dados em trânsito entre o serviço e outros AWS serviços integrados. Todos os dados que passam entre AWS Resilience Hub serviços integrados são criptografados usando Transport Layer Security (TLS). AWS Resilience Hub fornece ações pré-configuradas para tipos específicos de alvos em todos AWS os serviços e oferece suporte a ações para recursos de destino.

Identity and Access Management for AWS Resilience Hub

AWS Identity and Access Management (IAM) é uma ferramenta Serviço da AWS que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do AWS Resilience Hub. IAMé um Serviço da AWS que você pode usar sem custo adicional.

Tópicos

- Limitar as permissões para incluir ou excluir recomendações AWS Resilience Hub

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no AWS Resilience Hub.

Usuário do serviço — Se você usa o serviço AWS Resilience Hub para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do AWS Resilience Hub para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no AWS Resilience Hub, consulteSolução de problemas de identidade e acesso ao AWS Resilience Hub.

Administrador de serviços — Se você é responsável pelos recursos do AWS Resilience Hub em sua empresa, provavelmente tem acesso total ao AWS Resilience Hub. É seu trabalho determinar quais recursos e recursos do AWS Resilience Hub seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar o IAM AWS Resilience Hub, consulteComo o AWS Resilience Hub funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao AWS Resilience Hub. Para ver exemplos de políticas baseadas em identidade do AWS Resilience Hub que você pode usar, consulte. IAM Exemplos de políticas baseadas em identidade para AWS o Resilience Hub

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do 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 entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. 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 você mesmo assinar solicitações, consulte Assinar AWS API solicitações no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

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 ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um

conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no Guia do AWS IAM Identity Center usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários 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 IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. 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 IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter

informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .

- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- 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 do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações 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 FAS solicitações, consulte Encaminhar sessões de acesso.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de

propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. 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 Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando 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 JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar 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 do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente 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 Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM 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. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, 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 as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). 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 IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas 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. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços 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 atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

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 política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como o AWS Resilience Hub funciona com IAM

Antes de gerenciar o acesso IAM ao AWS Resilience Hub, saiba quais IAM recursos estão disponíveis para uso com o AWS Resilience Hub.

IAMrecursos que você pode usar com o AWS Resilience Hub

IAMrecurso	AWS Suporte do Resilience Hub
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC(tags nas políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim

Para ter uma visão geral de como o AWS Resilience Hub e outros AWS serviços funcionam com a maioria dos IAM recursos, consulte AWS os serviços que funcionam com IAM no Guia do IAMusuário.

Políticas baseadas em identidade para AWS o Resilience Hub

Compatível com políticas baseadas em identidade: Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas

controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para AWS o Resilience Hub

Para ver exemplos de políticas baseadas em identidade do AWS Resilience Hub, consulte. Exemplos de políticas baseadas em identidade para AWS o Resilience Hub

Políticas baseadas em recursos no Resilience AWS Hub

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um IAM administrador na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Ações políticas para o AWS Resilience Hub

Compatível com ações de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API 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 AWS Resilience Hub, consulte Ações definidas pelo AWS Resilience Hub na Referência de Autorização de Serviço.

As ações políticas no AWS Resilience Hub usam o seguinte prefixo antes da ação:

```
resiliencehub
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "resiliencehub:action1",
      "resiliencehub:action2"
         ]
```

Para ver exemplos de políticas baseadas em identidade do AWS Resilience Hub, consulte. Exemplos de políticas baseadas em identidade para AWS o Resilience Hub

Recursos políticos para o AWS Resilience Hub

Compatível com recursos de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (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 do AWS Resilience Hub e seusARNs, consulte Recursos definidos pelo AWS Resilience Hub na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo AWS Resilience Hub. ARN

Para ver exemplos de políticas baseadas em identidade do AWS Resilience Hub, consulte. Exemplos de políticas baseadas em identidade para AWS o Resilience Hub

Chaves de condição de política para o AWS Resilience Hub

Compatível com chaves de condição de política específicas de serviço: Sim

Os administradores podem usar AWS JSON políticas 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 `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, 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, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver

marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

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 IAM do usuário.

Para ver uma lista das chaves de condição do AWS Resilience Hub, consulte Chaves de condição do AWS Resilience Hub na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo AWS Resilience Hub.

Para ver exemplos de políticas baseadas em identidade do AWS Resilience Hub, consulte. Exemplos de políticas baseadas em identidade para AWS o Resilience Hub

ACLsno AWS Resilience Hub

SuportesACLs: Não

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

ABACcom o AWS Resilience Hub

Suportes ABAC (tags nas políticas): Parciais

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitos AWS recursos. Marcar entidades e recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

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 oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usando credenciais temporárias com o AWS Resilience Hub

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 esse trabalho IAM no Guia do IAM usuário.

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 a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. 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 emIAM.

Sessões de acesso direto para o AWS Resilience Hub

Suporta sessões de acesso direto (FAS): Sim

Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações 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 FAS solicitações, consulte Encaminhar sessões de acesso.

Funções de serviço do AWS Resilience Hub

Compatível com perfis de serviço: Sim

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do AWS Resilience Hub. Edite as funções de serviço somente quando o AWS Resilience Hub fornecer orientação para fazer isso.

Exemplos de políticas baseadas em identidade para AWS o Resilience Hub

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Resilience Hub. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte Criação de IAM políticas no Guia do IAMusuário.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AWS Resilience Hub, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição do AWS Resilience Hub na Referência de Autorização de Serviço. ARNs

Tópicos

- Melhores práticas de política
- Usando o console do AWS Resilience Hub
- Permitir que usuários visualizem suas próprias permissões
- Listando os AWS Resilience Hub aplicativos disponíveis

- Iniciando uma avaliação de inscrição
- Excluindo uma avaliação de aplicativo
- Criação de um modelo de recomendação para um aplicativo específico
- Excluindo um modelo de recomendação para um aplicativo específico
- Atualização de um aplicativo com uma política de resiliência específica

Melhores práticas de política

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

- Comece com políticas AWS gerenciadas e avance para permissões de privilégios mínimos — Para começar a conceder permissões para 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 AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas 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 usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica Serviço da AWS, como AWS CloudFormation. Para obter mais informações, consulte elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar

políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.

- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Usando o console do AWS Resilience Hub

Para acessar o console do AWS Resilience Hub, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do AWS Resilience Hub em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que eles estão tentando realizar.

Para garantir que usuários e funções ainda possam usar o console do AWS Resilience Hub, anexe também o AWS Resilience Hub `ConsoleAccess` ou a política `ReadOnly` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do IAM usuário.

A política a seguir concede aos usuários a permissão para listar e visualizar todos os recursos no AWS Resilience Hub console, mas não para criá-los, atualizá-los ou excluí-los.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "resiliencehub:List*",
                 "resiliencehub:Describe*"
             ],
```

```
            "Resource": "*"
        }
    ]
}
```

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Listando os AWS Resilience Hub aplicativos disponíveis

A política a seguir concede aos usuários permissão para listar os aplicativos do AWS Resilience Hub disponíveis.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Iniciando uma avaliação de inscrição

A política a seguir concede aos usuários a permissão para iniciar uma avaliação para um AWS Resilience Hub aplicativo específico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
```

```
}
```

Excluindo uma avaliação de aplicativo

A política a seguir concede aos usuários a permissão para excluir uma avaliação de um AWS Resilience Hub aplicativo específico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Criação de um modelo de recomendação para um aplicativo específico

A política a seguir concede aos usuários a permissão para criar um modelo de recomendação para um AWS Resilience Hub aplicativo específico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
```

```
}
```

Excluindo um modelo de recomendação para um aplicativo específico

A política a seguir concede aos usuários a permissão para excluir um modelo de recomendação para um AWS Resilience Hub aplicativo específico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Atualização de um aplicativo com uma política de resiliência específica

A política a seguir concede aos usuários a permissão para atualizar um aplicativo do AWS Resilience Hub com uma política de resiliência específica.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:UpdateApp"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ],
      "Condition": {
        "StringLike" : { "resiliencehub:policyArn" : "arn:aws:resiliencehub:us-
west-2:111122223333:resiliency-policy/*" }
```

```
        }
      }
    ]
  }
```

Configurar IAM funções e permissões

AWS Resilience Hub permite que você configure as IAM funções que você gostaria de usar ao executar avaliações para seu aplicativo. Há várias maneiras de configurar o AWS Resilience Hub para obter acesso somente de leitura aos recursos do seu aplicativo. No entanto, o AWS Resilience Hub recomenda as seguintes formas:

- Acesso baseado em função — Essa função é definida e usada na conta atual. AWS Resilience Hub assumirá essa função para acessar os recursos do seu aplicativo.

  Para fornecer acesso baseado em funções, a função deve incluir o seguinte:

  - Permissão somente de leitura para ler seus recursos (AWS Resilience Hub recomenda que você use a política `AWSResilienceHubAsssessmentExecutionPolicy` gerenciada).
  - Política de confiança para assumir essa função, o que permite que o Diretor de AWS Resilience Hub Serviço assuma essa função. Se você não tiver essa função configurada em sua conta, AWS Resilience Hub exibirá as instruções para criar essa função. Para obter mais informações, consulte the section called “Etapa 6: configurar permissões”.

  > **Note**
  >
  > Se você fornecer somente o nome da função de invocador e se seus recursos estiverem localizados em outra conta, AWS Resilience Hub usará esse nome de função nas outras contas para acessar os recursos entre contas. Opcionalmente, você pode configurar a função ARNs para outras contas, que serão usadas em vez do nome da função de invocador.

- Acesso IAM do usuário atual — AWS Resilience Hub usará o IAM usuário atual para acessar os recursos do seu aplicativo. Quando seus recursos estiverem em uma conta diferente, AWS Resilience Hub assumirá as seguintes IAM funções para acessar os recursos:

  - `AwsResilienceHubAdminAccountRole` na conta atual
  - `AwsResilienceHubExecutorAccountRole` em outras contas

Além disso, quando você configura uma avaliação agendada, AWS Resilience Hub assumirá a `AwsResilienceHubPeriodicAssessmentRole` função. No entanto, o uso não `AwsResilienceHubPeriodicAssessmentRole` é recomendado porque você deve configurar manualmente as funções e permissões, e algumas funcionalidades (como a notificação do Drift) podem não funcionar conforme o esperado.

Solução de problemas de identidade e acesso ao AWS Resilience Hub

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AWS Resilience Hub e. IAM

Tópicos

- Não estou autorizado a realizar uma ação no AWS Resilience Hub
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do AWS Resilience Hub

Não estou autorizado a realizar uma ação no AWS Resilience Hub

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre um *`my-example-widget`* recurso fictício, mas não tem as permissões fictícias`resiliencehub:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 resiliencehub:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `resiliencehub:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

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 AWS Resilience Hub.

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 IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação no AWS Resilience Hub. 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 AWS Resilience Hub

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AWS Resilience Hub oferece suporte a esses recursos, consulteComo o AWS Resilience Hub funciona com IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

AWS Resilience Hub referência de permissões de acesso

Você pode usar AWS Identity and Access Management (IAM) para gerenciar o acesso aos recursos do aplicativo e criar IAM políticas que se apliquem a usuários, grupos ou funções.

Cada AWS Resilience Hub aplicativo pode ser configurado para usar a the section called “Função do invocador” (uma IAM função) ou usar as permissões atuais IAM do usuário (junto com um conjunto de funções predefinidas para avaliação programada e entre contas). Nessa função, você pode anexar uma política que define as permissões necessárias AWS Resilience Hub para acessar outros AWS recursos ou recursos do aplicativo. A função de invocador deve ter uma política de confiança que seja adicionada ao AWS Resilience Hub Service Principal.

Para gerenciar as permissões do seu aplicativo, recomendamos o uso de the section called “AWS políticas gerenciadas”. É possível usar essas políticas gerenciadas sem modificações ou como um ponto de partida para escrever suas próprias políticas restritivas. Políticas podem restringir permissões de usuários no nível do recurso para ações diferentes usando condições adicionais.

Se os recursos do aplicativo estiverem em contas diferentes (contas secundárias/de recursos), você deverá configurar uma nova função em cada conta que contém os recursos do aplicativo.

Tópicos

- the section called “Usando a IAM função”
- the section called “Usando as permissões atuais IAM do usuário”

Usando a IAM função

AWS Resilience Hub usará uma IAM função predefinida existente para acessar seus recursos na conta principal ou na conta secundária/de recursos. Essa é a opção de permissão recomendada para acessar seus recursos.

Tópicos

- the section called “Função do invocador”
- the section called “Funções em AWS contas diferentes para acesso entre contas”

Função do invocador

A função de AWS Resilience Hub invocador é uma função AWS Identity and Access Management (IAM) que AWS Resilience Hub pressupõe acessar AWS serviços e recursos. Por exemplo, você pode criar uma função de invocador que tenha permissão para acessar seu CFN modelo e o recurso que ele cria. Esta página fornece informações sobre como criar, visualizar e gerenciar uma função de invocador de aplicativo.

Ao criar um aplicativo, você fornece uma função de invocador. O AWS Resilience Hub assume essa função para acessar seus recursos quando você importa recursos ou inicia uma avaliação. AWS Resilience Hub Para assumir adequadamente sua função de invocador, a política de confiança da função deve especificar o principal do AWS Resilience Hub serviço (resiliencehub.amazonaws.com) como um serviço confiável.

Para visualizar a função de invocador do aplicativo, escolha Aplicativos no painel de navegação e, em seguida, escolha Atualizar permissões no menu Ações na página Aplicativo.

É possível adicionar ou remover permissões de uma função de invocador de aplicativo a qualquer momento ou configurar seu aplicativo para usar uma função diferente para acessar recursos do aplicativo.

Tópicos

- the section called “Criando uma função de invocador no console IAM”
- the section called “Gerenciando funções com o IAM API”
- the section called “Definindo a política de confiança usando o JSON arquivo”

Criando uma função de invocador no console IAM

AWS Resilience Hub Para permitir o acesso a AWS serviços e recursos, você deve criar uma função de invocador na conta principal usando o IAM console. Para obter mais informações sobre a criação de funções usando o IAM console, consulte Criação de uma função para um AWS serviço (console).

Para criar uma função de invocador na conta principal usando o console IAM

1. Abra o console do IAM em `https://console.aws.amazon.com/iam/`.
2. No painel de navegação, escolha Funções e então escolha Criar função.
3. Selecione Política de confiança personalizada, copie a política a seguir na janela Política de confiança personalizada e escolha Avançar.

> **Note**
>
> Se seus recursos estiverem em contas diferentes, você precisará criar uma função em cada uma dessas contas e usar a política de confiança da conta secundária para as outras contas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Na seção Políticas de permissões da página Adicionar permissões, insira `AWSResilienceHubAsssessmentExecutionPolicy` na caixa Filtrar políticas por propriedade ou nome da política e pressione enter.
5. Selecione a política e escolha Próximo.
6. Na seção Detalhes da função, insira um nome de função exclusivo (como `AWSResilienceHubAssessmentRole`) na caixa Nome da função.

   Esse campo aceita somente caracteres alfanuméricos e '`+=,.@-_/`'.
7. (Opcional) Na caixa Descrição, insira uma descrição para a função.
8. Selecione Criar função.

Para editar os casos de uso e as permissões, na Etapa 6, escolha o botão Editar que está localizado à direita nas seções Etapa 1: selecionar entidades confiáveis ou Etapa 2: adicionar permissões.

Depois de criar a função de invocador e a função de recurso (se aplicável), você pode configurar seu aplicativo para usar essas funções.

> **Note**
>
> Você deve ter uma `iam:passRole` permissão em seu IAM usuário/função atual para a função de invocador ao criar ou atualizar o aplicativo. No entanto, você não precisa dessa permissão para executar uma avaliação.

Gerenciando funções com o IAM API

A política de confiança de uma função concede a permissão ao principal especificado para assumir a função. Para criar as funções usando AWS Command Line Interface (AWS CLI), use o `create-role` comando. Ao usar esse comando, é possível especificar a política de confiança em linha. O exemplo a seguir mostra como conceder ao AWS Resilience Hub serviço a permissão principal para assumir sua função.

> **Note**
>
> O requisito para escapar de aspas (`'  '`) na JSON string pode variar com base na sua versão do shell.

Exemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{
  "Version": "2012-10-17","Statement":
  [
    {
      "Effect": "Allow",
      "Principal": {"Service": "resiliencehub.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}'
```

Definindo a política de confiança usando o JSON arquivo

Você pode definir a política de confiança para a função usando um JSON arquivo separado e, em seguida, executar o `create-role` comando. No exemplo a seguir, **`trust-policy.json`** é um arquivo que contém a política de confiança no diretório atual. Essa política é anexada a uma função por meio da execução de um comando **`create-role`**. A saída do comando **`create-role`** é mostrada no Exemplo de saída. Para adicionar permissões à função, use o attach-policy-to-rolecomando e comece adicionando a política `AWSResilienceHubAsssessmentExecutionPolicy` gerenciada. Para obter mais informações sobre esta política gerenciada, consulte the section called "AWSResilienceHubAsssessmentExecutionPolicy".

Exemplo de **`trust-policy.json`**

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "resiliencehub.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }]
}
```

Exemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-
role-policy-document file://trust-policy.json
```

Exemplo de saída

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole",
        "CreateDate": "2020-01-17T23:19:12Z",
```

```
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [{
                "Effect": "Allow",
                "Principal": {
                    "Service": "resiliencehub.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }]
        }
    }
}
```

Exemplo de **`attach-policy-to-role`**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

Funções em AWS contas diferentes para acesso entre contas - opcional

Quando seus recursos estão localizados em contas secundárias/de recursos, você deve criar funções em cada uma dessas contas AWS Resilience Hub para permitir a avaliação bem-sucedida do seu aplicativo. O procedimento de criação da função é semelhante ao processo de criação da função do invocador, exceto pela configuração da política de confiança.

> **Note**
>
> Você deve criar as funções nas contas secundárias em que os recursos estão localizados.

Tópicos

- the section called “Criação de uma função no IAM console para contas secundárias/de recursos”
- the section called “Gerenciando funções com o IAM API”
- the section called “Definindo a política de confiança usando o JSON arquivo”

Criação de uma função no IAM console para contas secundárias/de recursos

AWS Resilience Hub Para permitir o acesso a AWS serviços e recursos em outras AWS contas, você deve criar funções em cada uma dessas contas.

Para criar uma função no IAM console para as contas secundárias/de recursos usando o console IAM

1. Abra o console do IAM em `https://console.aws.amazon.com/iam/`.
2. No painel de navegação, escolha Funções e então escolha Criar função.
3. Selecione Política de confiança personalizada, copie a política a seguir na janela Política de confiança personalizada e escolha Avançar.

> **Note**
>
> Se seus recursos estiverem em contas diferentes, você precisará criar uma função em cada uma dessas contas e usar a política de confiança da conta secundária para as outras contas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Na seção Políticas de permissões da página Adicionar permissões, insira `AWSResilienceHubAsssessmentExecutionPolicy` na caixa Filtrar políticas por propriedade ou nome da política e pressione enter.
5. Selecione a política e escolha Próximo.
6. Na seção Detalhes da função, insira um nome de função exclusivo (como `AWSResilienceHubAssessmentRole`) na caixa Nome da função.
7. (Opcional) Na caixa Descrição, insira uma descrição para a função.
8. Selecione Criar função.

Para editar os casos de uso e as permissões, na Etapa 6, escolha o botão Editar que está localizado à direita nas seções Etapa 1: selecionar entidades confiáveis ou Etapa 2: adicionar permissões.

Além disso, você também precisa adicionar a permissão `sts:assumeRole` à função de invocador para permitir que ela assuma as funções em suas contas secundárias.

Adicione a seguinte política à sua função de invocador para cada uma das funções secundárias que você criou:

```
{
    "Effect": "Allow",
    "Resource": [
      "arn:aws:iam::secondary_account_id_1:role/RoleInSecondaryAccount_1",
      "arn:aws:iam::secondary_account_id_2:role/RoleInSecondaryAccount_2",
      ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
}
```

Gerenciando funções com o IAM API

A política de confiança de uma função concede a permissão ao principal especificado para assumir a função. Para criar as funções usando AWS Command Line Interface (AWS CLI), use o `create-role` comando. Ao usar esse comando, é possível especificar a política de confiança em linha. O exemplo a seguir mostra como conceder permissão ao responsável pelo AWS Resilience Hub serviço para assumir sua função.

> **Note**
>
> O requisito para escapar de aspas (`'  '`) na JSON string pode variar com base na sua versão do shell.

Exemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{"Version": "2012-10-17","Statement": [{"Effect": "Allow","Principal":
 {"AWS": ["arn:aws:iam::primary_account_id:role/InvokerRoleName"]},"Action":
 "sts:AssumeRole"}]}'
```

Você também pode definir a política de confiança para a função usando um JSON arquivo separado. No exemplo a seguir, `trust-policy.json` é um arquivo no diretório atual.

Definindo a política de confiança usando o JSON arquivo

Você pode definir a política de confiança para a função usando um JSON arquivo separado e, em seguida, executar o `create-role` comando. No exemplo a seguir, **`trust-policy.json`** é um arquivo que contém a política de confiança no diretório atual. Essa política é anexada a uma função por meio da execução de um comando **`create-role`**. A saída do comando **`create-role`** é mostrada no Exemplo de saída. Para adicionar permissões a uma função, use o attach-policy-to-rolecomando e comece adicionando a política `AWSResilienceHubAsssessmentExecutionPolicy` gerenciada. Para obter mais informações sobre esta política gerenciada, consulte the section called "AWSResilienceHubAsssessmentExecutionPolicy".

Exemplo de **`trust-policy.json`**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Exemplo de **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document file://trust-policy.json
```

Exemplo de saída

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole2",
        "RoleId": "AROAT2GICMEDJML6EVQRG",
        "Arn": "arn:aws:iam::262412591366:role/AWSResilienceHubAssessmentRole2",
        "CreateDate": "2023-08-02T07:49:23+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": [
                            "arn:aws:iam::262412591366:role/
AWSResilienceHubAssessmentRole"
                        ]
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Exemplo de **`attach-policy-to-role`**

`aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --policy-arn arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`.

Usando as permissões atuais IAM do usuário

Use esse método se quiser usar suas permissões de IAM usuário atuais para criar e executar uma avaliação. Você pode anexar a política `AWSResilienceHubAsssessmentExecutionPolicy` gerenciada ao seu IAM usuário ou a uma função associada ao seu usuário.

Configuração de conta única

Usar a política gerenciada mencionada acima é suficiente para executar uma avaliação em um aplicativo que é gerenciado na mesma conta do IAM usuário.

Configuração de avaliação programada

Você deve criar uma nova função `AwsResilienceHubPeriodicAssessmentRole` para permitir que o AWS Resilience Hub execute as tarefas programadas relacionadas à avaliação.

> **Note**
>
> - Ao usar o acesso baseado em função (com a função de invocador mencionada acima), essa etapa não é necessária.
> - O tipo de função deve ser `AwsResilienceHubPeriodicAssessmentRole`.

Para permitir AWS Resilience Hub a execução de tarefas programadas relacionadas à avaliação

1. Anexe a política gerenciada `AWSResilienceHubAsssessmentExecutionPolicy` à função.
2. Adicione a política a seguir, onde `primary_account_id` está a AWS conta em que o aplicativo está definido e executará a avaliação. Além disso, você deve adicionar a política de confiança associada à função da avaliação agendada, (`AwsResilienceHubPeriodicAssessmentRole`), que dá permissões para que o AWS Resilience Hub serviço assuma a função da avaliação agendada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAdminAccountRole"
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAssessmentEKSAccessRole"
      ]
    }
  ]
}
```

Política de confiança para a função da avaliação programada (**`AwsResilienceHubPeriodicAssessmentRole`**)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Configuração entre contas

As políticas de IAM permissões a seguir são necessárias se você estiver usando o AWS Resilience Hub com várias contas. Cada AWS conta pode precisar de permissões diferentes, dependendo do seu caso de uso. Ao configurar o AWS Resilience Hub para acesso entre contas, as seguintes contas e funções são consideradas:

- Conta principal: conta da AWS na qual você deseja criar o aplicativo e executar avaliações.
- Conta (s) secundária/de recursos — AWS conta (s) em que os recursos estão localizados.

> **Note**
>
> - Ao usar o acesso baseado em função (com a função de invocador mencionada acima), essa etapa não é necessária.
> - Para obter mais informações sobre a configuração de permissões para acessar o Amazon Elastic Kubernetes Service, consulte the section called "Habilitando o AWS Resilience Hub acesso ao seu EKS cluster da Amazon".

Configuração da conta principal

Você deve criar uma nova função `AwsResilienceHubAdminAccountRole` na conta principal e habilitar o AWS Resilience Hub acesso para assumi-la. Essa função será usada para acessar outra função em sua AWS conta que contém seus recursos. Ela não deve ter permissões para ler recursos.

> **Note**
>
> - O tipo de função deve ser `AwsResilienceHubAdminAccountRole`.
> - Ela deve ser criada na conta principal.
> - Seu IAM usuário/função atual deve ter `iam:assumeRole` permissão para assumir essa função.
> - Substitua `secondary_account_id_1/2/...` pelos identificadores de conta secundários relevantes.

A política a seguir fornece permissões de executor à sua função para acessar recursos em outra função em sua AWS conta:

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::secondary_account_id_1:role/AwsResilienceHubExecutorAccountRole",
```

```
        "arn:aws:iam::secondary_account_id_2:role/AwsResilienceHubExecutorAccountRole",
        ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

A política de confiança para a função de administrador (`AwsResilienceHubAdminAccountRole`) é a seguinte:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubPeriodicAssessmentRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Configuração de conta(s) secundária/de recursos

Em cada uma de suas contas secundárias, você deve criar uma nova `AwsResilienceHubExecutorAccountRole` e habilitar a função de administrador criada acima para assumir essa função. Como essa função será usada AWS Resilience Hub para verificar e avaliar os recursos do seu aplicativo, ela também exigirá as permissões apropriadas.

No entanto, você deve anexar a política gerenciada `AWSResilienceHubAsssessmentExecutionPolicy` à função e anexar a política de função do executor.

A política de confiança da função do executor é a seguinte:

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS políticas gerenciadas para AWS Resilience Hub

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 políticas gerenciadas pelo cliente da específicas para seus casos de uso.

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

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

AWSResilienceHubAsssessmentExecutionPolicy

Você pode anexar o `AWSResilienceHubAsssessmentExecutionPolicy` às suas IAM identidades. Ao executar uma avaliação, essa política concede permissões de acesso a outros AWS serviços para a execução de avaliações.

Detalhes de permissões

Essa política fornece permissões adequadas para publicar alarmes AWS FIS e SOP modelos em seu bucket do Amazon Simple Storage Service (Amazon S3). O nome do bucket do Amazon S3 deve começar com `aws-resilience-hub-artifacts-`. Se você quiser publicar em outro bucket do Amazon S3, você pode fazer isso durante a chamada. `CreateRecommendationTemplate` API Para obter mais informações, consulte CreateRecommendationTemplate.

Esta política inclui as seguintes permissões:

- Amazon CloudWatch (CloudWatch) — Obtém todos os alarmes implementados que você configurou na Amazon CloudWatch para monitorar o aplicativo. Além disso, usamos `cloudwatch:PutMetricData` para publicar CloudWatch métricas para a pontuação de resiliência do aplicativo no `ResilienceHub` namespace.
- Amazon Data Lifecycle Manager — Obtém e fornece `Describe` permissões para os recursos do Amazon Data Lifecycle Manager associados à sua conta. AWS
- Amazon DevOps Guru — Lista e fornece `Describe` permissões para os recursos do Amazon DevOps Guru associados à sua AWS conta.
- Amazon DocumentDB — Lista e fornece `Describe` permissões para recursos do Amazon DocumentDB associados à sua conta. AWS
- Amazon DynamoDB (DynamoDB): lista e fornece permissões `Describe` para recursos do Amazon DynamoDB associados à sua conta da AWS .
- Amazon ElastiCache (ElastiCache) — Fornece `Describe` permissões para ElastiCache recursos associados à sua AWS conta.
- Amazon Elastic Compute Cloud (AmazonEC2) — Lista e fornece `Describe` permissões para EC2 recursos da Amazon associados à sua AWS conta.
- Amazon Elastic Container Registry (AmazonECR) — Fornece `Describe` permissões para ECR recursos da Amazon associados à sua AWS conta.
- Amazon Elastic Container Service (AmazonECS) — Fornece `Describe` permissões para ECS recursos da Amazon associados à sua AWS conta.

- Amazon Elastic File System (AmazonEFS) — Fornece `Describe` permissões para EFS recursos da Amazon associados à sua AWS conta.
- Amazon Elastic Kubernetes Service (EKSAmazon) — Lista e `Describe` fornece permissões para recursos EKS da Amazon associados à sua conta. AWS
- Amazon EC2 Auto Scaling — Lista e fornece `Describe` permissões para recursos do Amazon EC2 Auto Scaling associados à sua conta. AWS
- Amazon EC2 Systems Manager (SSM) — Fornece `Describe` permissões para SSM recursos associados à sua AWS conta.
- Amazon Fault Injection Service (AWS FIS) — Lista e fornece `Describe` permissões para AWS FIS experimentos e modelos de experimentos associados à sua AWS conta.
- Amazon FSx para Windows File Server (AmazonFSx) — Lista e fornece `Describe` permissões para FSx recursos da Amazon associados à sua AWS conta.
- Amazon RDS — Lista e fornece `Describe` permissões para RDS recursos da Amazon associados à sua AWS conta.
- Amazon Route 53 (Route 53): lista e fornece permissões `Describe` para recursos do Route 53 associados à sua conta da AWS .
- Amazon Route 53 Resolver — Lista e fornece `Describe` permissões para Amazon Route 53 Resolver recursos associados à sua AWS conta.
- Amazon Simple Notification Service (AmazonSNS) — Lista e fornece `Describe` permissões para SNS recursos da Amazon associados à sua AWS conta.
- Amazon Simple Queue Service (AmazonSQS) — Lista e fornece `Describe` permissões para SQS recursos da Amazon associados à sua AWS conta.
- Amazon Simple Storage Service (Amazon S3) — Lista e `Describe` fornece permissões para recursos do Amazon S3 associados à sua conta. AWS

> **Note**
>
> Ao executar uma avaliação, se houver alguma permissão ausente que precise ser atualizada a partir das políticas gerenciadas, AWS Resilience Hub concluirá com êxito a avaliação usando s3: GetBucketLogging permission. No entanto, AWS Resilience Hub exibirá uma mensagem de aviso que lista as permissões ausentes e fornecerá um período de carência para adicioná-las. Se você não adicionar as permissões ausentes dentro do período de carência especificado, a avaliação falhará.

- AWS Backup — Lista e obtém `Describe` permissões para os recursos do Amazon EC2 Auto Scaling associados à sua AWS conta.
- AWS CloudFormation — Lista e obtém `Describe` permissões para recursos em AWS CloudFormation pilhas associadas à sua AWS conta.
- AWS DataSync — Lista e fornece `Describe` permissões para AWS DataSync recursos associados à sua AWS conta.
- AWS Directory Service — Lista e fornece `Describe` permissões para AWS Directory Service recursos associados à sua AWS conta.
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery) — Fornece `Describe` permissões para recursos do Elastic Disaster Recovery associados à sua AWS conta.
- AWS Lambda (Lambda) — Lista e fornece `Describe` permissões para recursos do Lambda associados à sua conta. AWS
- AWS Resource Groups (Resource Groups) — Lista e fornece `Describe` permissões para recursos de Resource Groups associados à sua AWS conta.
- AWS Service Catalog (Service Catalog) — Lista e fornece `Describe` permissões para recursos do Service Catalog associados à sua AWS conta.
- AWS Step Functions — Lista e fornece `Describe` permissões para AWS Step Functions recursos associados à sua AWS conta.
- Elastic Load Balancing — Lista e fornece `Describe` permissões para recursos do Elastic Load Balancing associados à sua conta. AWS
- `ssm:GetParametersByPath`— Usamos essa permissão para gerenciar CloudWatch alarmes, testes ou SOPs que estejam configurados para seu aplicativo.

A IAM política a seguir é necessária para que uma AWS conta adicione permissões para usuários, grupos de usuários e funções que forneçam as permissões necessárias para que sua equipe acesse AWS os serviços durante a execução das avaliações.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSResilienceHubFullResourceStatement",
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:DescribeScalableTargets",
                "autoscaling:DescribeAutoScalingGroups",
```

```
                "backup:DescribeBackupVault",
                "backup:GetBackupPlan",
                "backup:GetBackupSelection",
                "backup:ListBackupPlans",
                "backup:ListBackupSelections",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "datasync:DescribeTask",
                "datasync:ListLocations",
                "datasync:ListTasks",
                "devops-guru:ListMonitoredResources",
                "dlm:GetLifecyclePolicies",
                "dlm:GetLifecyclePolicy",
                "docdb-elastic:GetCluster",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:ListTagsForResource",
                "drs:DescribeJobs",
                "drs:DescribeSourceServers",
                "drs:GetReplicationConfiguration",
                "ds:DescribeDirectories",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:DescribeGlobalTable",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTagsOfResource",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeFleets",
                "ec2:DescribeHosts",
                "ec2:DescribeInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcEndpoints",
```

```
                "ecr:DescribeRegistry",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeClusters",
                "ecs:DescribeContainerInstances",
                "ecs:DescribeServices",
                "ecs:DescribeTaskDefinition",
                "ecs:ListContainerInstances",
                "ecs:ListServices",
                "eks:DescribeCluster",
                "eks:DescribeFargateProfile",
                "eks:DescribeNodegroup",
                "eks:ListFargateProfiles",
                "eks:ListNodegroups",
                "elasticache:DescribeCacheClusters",
                "elasticache:DescribeGlobalReplicationGroups",
                "elasticache:DescribeReplicationGroups",
                "elasticache:DescribeSnapshots",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "fis:GetExperimentTemplate",
                "fis:ListExperimentTemplates",
                "fis:ListExperiments",
                "fsx:DescribeFileSystems",
                "lambda:GetFunctionConcurrency",
                "lambda:GetFunctionConfiguration",
                "lambda:ListAliases",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctionEventInvokeConfigs",
                "lambda:ListVersionsByFunction",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeDBProxies",
                "rds:DescribeDBProxyTargets",
                "rds:DescribeDBSnapshots",
                "rds:DescribeGlobalClusters",
                "rds:ListTagsForResource",
```

```
                "resource-groups:GetGroup",
                "resource-groups:ListGroupResources",
                "route53-recovery-control-config:ListClusters",
                "route53-recovery-control-config:ListControlPanels",
                "route53-recovery-control-config:ListRoutingControls",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:ListBucket",
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources",
                "sns:GetSubscriptionAttributes",
                "sns:GetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sqs:GetQueueAttributes",
                "sqs:GetQueueUrl",
                "ssm:DescribeAutomationExecutions",
                "states:DescribeStateMachine",
                "states:ListStateMachineVersions",
                "states:ListStateMachineAliases",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSResilienceHubApiGatewayStatement",
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/apis/*",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/usageplans"
            ]
        },
        {
            "Sid": "AWSResilienceHubS3ArtifactStatement",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubS3AccessStatement",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetMultiRegionAccessPointRoutes",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubCloudWatchStatement",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "cloudwatch:namespace": "ResilienceHub"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubSSMStatement",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
        }
    ]
}
```

AWS Resilience Hub atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Resilience Hub desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o RSS feed na página Histórico do AWS Resilience Hub documento.

Alteração	Descrição	Data
AWSResilienceHubAssessmentExecutionPolicy—Mudança	AWS Resilience Hub atualizado `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permissões para permitir que você acesse recursos e configurações no Amazon DocumentDB, no Elastic Load Balancing AWS Lambda e durante a execução de avaliações.	01 de agosto de 2024
AWSResilienceHubAssessmentExecutionPolicy—Mudança	AWS Resilience Hub atualizado `AWSResilienceHubAssessmentExecution`	26 de março de 2024

Alteração	Descrição	Data
	`Policy` para conceder `Describe` permissões para permitir que você leia a configuração do Amazon FSx para Windows File Server enquanto executa avaliações.	
AWSResilienceHubAssessmentExecutionPolicy—Mudança	AWS Resilience Hub atualizado `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permissões para permitir que você leia a AWS Step Functions configuração durante a execução das avaliações.	30 de outubro de 2023
AWSResilienceHubAssessmentExecutionPolicy—Mudança	AWS Resilience Hub atualizado `AWSResilienceHubAssessmentExecutionPolicy` para conceder `Describe` permissões para permitir que você acesse recursos na Amazon RDS enquanto executa avaliações.	5 de outubro de 2023
AWSResilienceHubAssessmentExecutionPolicy—Novo	Essa AWS Resilience Hub política fornece acesso a outros AWS serviços para a execução de avaliações.	26 de junho de 2023
AWS Resilience Hub começou a rastrear alterações	AWS Resilience Hub começou a rastrear as mudanças em suas políticas AWS gerenciadas.	15 de junho de 2023

AWS Resilience Hub referência de personas e IAM permissões

Você pode conceder as IAM permissões às pessoas com AWS Resilience Hub as quais é necessário trabalhar usando a política `AWSResilienceHubAsssessmentExecutionPolicy` AWS gerenciada e uma das seguintes políticas específicas para cada pessoa. Para obter mais informações sobre a política AWS gerenciada, consultethe section called "AWSResilienceHubAsssessmentExecutionPolicy".

Políticas para personas sugeridas por: AWS Resilience Hub

- IAMpermissões para a persona do gerenciador de aplicativos de infraestrutura
- IAMpermissões para a persona de gerente de continuidade de negócios
- IAMpermissões para a persona do proprietário do aplicativo
- IAMpermissões para conceder acesso somente para leitura

IAMpermissões para a persona do gerenciador de aplicativos de infraestrutura

A política a seguir concede as permissões necessárias para a personalidade do gerente de aplicativos de infraestrutura.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InfrastructureApplicationManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
```

```
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource"
      ],
      "Resource": "*"
    }
  ]
}
```

IAMpermissões para a persona de gerente de continuidade de negócios

A política a seguir concede as permissões necessárias para a personalidade de gerente de continuidade de negócios.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BusinessContinuityManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

IAMpermissões para a persona do proprietário do aplicativo

A política a seguir concede as permissões necessárias para a personalidade do proprietário do aplicativo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ApplicationOwner",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:BatchUpdateRecommendationStatus",
        "resiliencehub:CreateApp",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteApp",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:ImportResourcesToDraftAppVersion",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateApp",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

IAMpermissões para conceder acesso somente para leitura

A política a seguir concede as permissões necessárias para acesso somente leitura.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Importando o arquivo de estado do Terraform para AWS Resilience Hub

AWS Resilience Hub suporta a importação de arquivos de estado do Terraform que são criptografados usando criptografia do lado do servidor () SSE com chaves gerenciadas do Amazon Simple Storage Service (SSE-S3) ou com chaves gerenciadas (-). AWS Key Management Service SSE KMS Se seus arquivos de estado do Terraform forem criptografados usando chaves de criptografia fornecidas pelo cliente (SSE-C), você não poderá importá-los usando. AWS Resilience Hub

A importação de arquivos de estado do Terraform AWS Resilience Hub requer as seguintes IAM políticas, dependendo de onde seu arquivo de estado está localizado.

Importar arquivos de estado do Terraform de um bucket do Amazon S3 localizado na conta principal

A seguinte política e IAM política de bucket do Amazon S3 são necessárias para permitir acesso de AWS Resilience Hub leitura aos seus arquivos de estado do Terraform localizados em um bucket do Amazon S3 na conta principal.

- Política de bucket: uma política de bucket no bucket de destino do Amazon S3, que está localizado na conta principal. Para obter mais informações, veja o exemplo a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

- Política de identidade — A política de identidade associada à função de invocador definida para esse aplicativo ou a IAM função AWS atual AWS Resilience Hub na conta principal AWS . Para obter mais informações, veja o exemplo a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

> **Note**
>
> Se você estiver usando a política gerenciada `AWSResilienceHubAsssessmentExecutionPolicy`, a permissão `ListBucket` não é necessária.

> **Note**
>
> Se seus arquivos de estado do Terraform forem criptografados usandoKMS, você deverá adicionar a seguinte `kms:Decrypt` permissão.
>
> ```
> {
>  "Effect": "Allow",
>  "Action": [
>  "kms:Decrypt",
>  ],
>  "Resource": "<arn_of_kms_key>"
> }
> ```

Importando arquivos de estado do Terraform de um bucket do Amazon S3 localizado em uma conta secundária

- Política de bucket: uma política de bucket no bucket Amazon S3 de destino, que está localizado em uma das contas secundárias. Para obter mais informações, veja o exemplo a seguir.

```
 {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

- Política de identidade — A política de identidade associada à função da AWS conta, que está sendo AWS Resilience Hub executada na AWS conta principal. Para obter mais informações, veja o exemplo a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

> **Note**
>
> Se você estiver usando a política gerenciada `AWSResilienceHubAsssessmentExecutionPolicy`, a permissão `ListBucket` não é necessária.

> **Note**
>
> Se seus arquivos de estado do Terraform forem criptografados usandoKMS, você deverá adicionar a seguinte `kms:Decrypt` permissão.
>
> ```
> {
>  "Effect": "Allow",
>  "Action": [
>  "kms:Decrypt",
>  ],
>  "Resource": "<arn_of_kms_key>"
> }
> ```

Habilitando o AWS Resilience Hub acesso ao seu cluster do Amazon Elastic Kubernetes Service

AWS Resilience Hub avalia a resiliência de um cluster do Amazon Elastic Kubernetes Service EKS (Amazon) analisando a infraestrutura do seu cluster Amazon. EKS AWS Resilience Hub usa a configuração de controle de acesso (RBAC) baseado em funções do Kubernetes para avaliar outras cargas de trabalho do Kubernetes (K8s), que são implantadas como parte do cluster da Amazon. EKS AWS Resilience Hub Para consultar seu EKS cluster da Amazon para analisar e avaliar a carga de trabalho, você deve concluir o seguinte:

- Crie ou use uma função existente AWS Identity and Access Management (IAM) na mesma conta do EKS cluster da Amazon.
- Permita o acesso de IAM usuários e funções ao seu EKS cluster da Amazon e conceda permissões adicionais somente de leitura aos recursos K8s dentro do cluster da Amazon. EKS Para obter mais informações sobre como habilitar o acesso de IAM usuários e funções ao seu EKS cluster da Amazon, consulte Habilitando o acesso de IAM usuários e funções ao seu cluster - Amazon EKS.

O acesso ao seu EKS cluster da Amazon usando IAM entidades é habilitado pelo AWS IAMAuthenticator for Kubernetes, que é executado no plano de controle da Amazon. EKS O autenticador obtém suas informações de configuração de `aws-auth ConfigMap`.

> **Note**
>
> - Para obter mais informações sobre todas as `aws-auth ConfigMap` configurações, consulte Formato de configuração completo ativado GitHub.
> - Para obter mais informações sobre IAM identidades diferentes, consulte Identidades (usuários, grupos e funções) no Guia do IAM usuário.
> - Para obter mais informações sobre a configuração do controle de acesso (RBAC) baseado em função do Kubernetes, consulte Como usar a autorização. RBAC

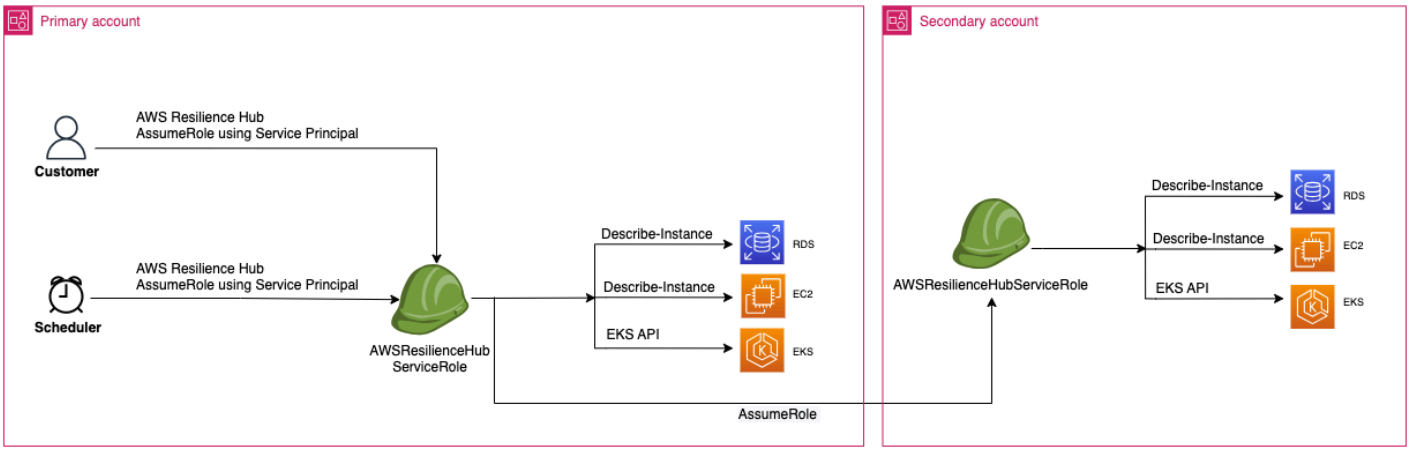
AWS Resilience Hub consulta recursos dentro do seu EKS cluster da Amazon usando uma IAM função na sua conta. AWS Resilience Hub Para acessar recursos dentro do seu EKS cluster da Amazon, a IAM função usada por AWS Resilience Hub deve ser mapeada para um grupo

Kubernetes com permissões suficientes de somente leitura para os recursos dentro do seu cluster da Amazon. EKS

AWS Resilience Hub permite acessar seus recursos de EKS cluster da Amazon usando uma das seguintes opções de IAM função:

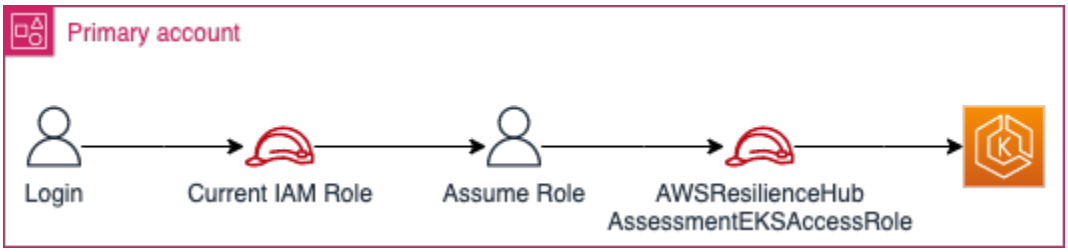
- Se seu aplicativo estiver configurado para usar acesso baseado em funções para acessar recursos, a função de invocador ou a função de conta secundária transmitida AWS Resilience Hub durante a criação de um aplicativo será usada para acessar seu cluster da Amazon EKS durante a avaliação.

  O diagrama conceitual a seguir mostra como AWS Resilience Hub acessa os EKS clusters da Amazon quando o aplicativo é configurado como um aplicativo baseado em funções.

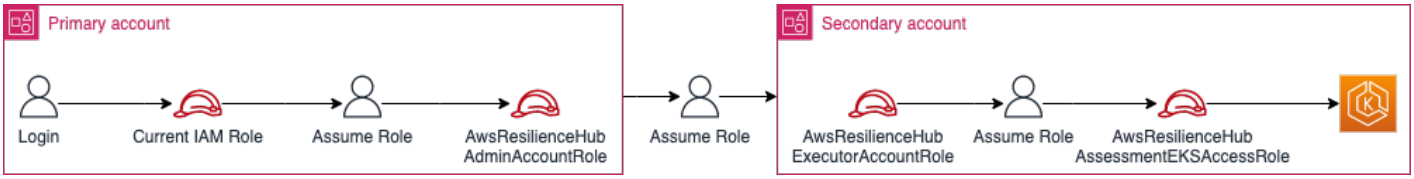


- Se seu aplicativo estiver configurado para usar o IAM usuário atual para acessar o recurso, você deverá criar uma nova IAM função com o nome `AwsResilienceHubAssessmentEKSAccessRole` na mesma conta do EKS cluster da Amazon. Essa IAM função será então usada para acessar seu EKS cluster da Amazon.

  O diagrama conceitual a seguir mostra como AWS Resilience Hub acessa os EKS clusters da Amazon implantados em sua conta principal quando o aplicativo está configurado para usar as permissões atuais IAM do usuário.



O diagrama conceitual a seguir mostra como AWS Resilience Hub acessa os EKS clusters da Amazon implantados em uma conta secundária quando o aplicativo está configurado para usar as permissões atuais IAM do usuário.



Concedendo AWS Resilience Hub acesso aos recursos em seu cluster da Amazon EKS

AWS Resilience Hub permite que você acesse recursos localizados nos EKS clusters da Amazon, desde que você tenha configurado as permissões necessárias.

Conceder as permissões necessárias AWS Resilience Hub para descobrir e avaliar recursos dentro do cluster da Amazon EKS

1. Configure uma IAM função para acessar o EKS cluster da Amazon.

   Se você configurou seu aplicativo usando o acesso baseado em função, você pode pular esta etapa e prosseguir para a etapa 2 e usar a função que você usou para criar o aplicativo. Para obter mais informações sobre como AWS Resilience Hub usa IAM funções, consultethe section called “Como o AWS Resilience Hub funciona com IAM”.

   Se você configurou seu aplicativo usando as permissões de IAM usuário atuais, você deve criar uma `AwsResilienceHubAssessmentEKSAccessRole` IAM função na mesma conta do EKS cluster da Amazon. Essa IAM função será então usada ao acessar seu EKS cluster da Amazon.

   Ao importar e avaliar seu aplicativo, AWS Resilience Hub usa uma IAM função para acessar os recursos em seu cluster da AmazonEKS. Essa função deve ser criada na mesma conta do seu EKS cluster da Amazon e será mapeada com um grupo Kubernetes que inclui as permissões exigidas AWS Resilience Hub para avaliar seu cluster da Amazon. EKS

   Se o seu EKS cluster da Amazon estiver na mesma conta da conta de AWS Resilience Hub chamada, a função deverá ser criada usando a seguinte política de IAM confiança. Nesta política de IAM confiança, `caller_IAM_role` é usado na conta corrente APIs para solicitar AWS Resilience Hub.

> **Note**
>
> Essa `caller_IAM_role` é a função associada à sua conta de AWS usuário.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Se o seu EKS cluster da Amazon estiver em uma conta cruzada (uma conta diferente da conta de AWS Resilience Hub chamada), você deverá criar a `AwsResilienceHubAssessmentEKSAccessRole` IAM função usando a seguinte política de IAM confiança:

> **Note**
>
> Como pré-requisito, para acessar o EKS cluster da Amazon que está implantado em uma conta diferente da conta do AWS Resilience Hub usuário, você deve configurar o acesso de várias contas. Para obter mais informações, consulte

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/
AwsResilienceHubExecutorRole"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Crie `ClusterRole` e `ClusterRoleBinding` (ou`RoleBinding`) funções para o AWS Resilience Hub aplicativo.

   `ClusterRoleBinding`Criará `ClusterRole` e concederá as permissões de somente leitura necessárias AWS Resilience Hub para analisar e avaliar recursos que fazem parte de determinados namespaces em seu cluster da Amazon. EKS

   AWS Resilience Hub permite que você limite o acesso aos seus namespaces para gerar avaliações de resiliência preenchendo uma das seguintes opções:

   a. Conceda acesso de leitura em todos os namespaces ao aplicativo do AWS Resilience Hub .

      AWS Resilience Hub Para avaliar a resiliência dos recursos em todos os namespaces em um EKS cluster da Amazon, você deve criar o seguinte e. `ClusterRole` `ClusterRoleBinding`

      - `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — Define as permissões necessárias AWS Resilience Hub para avaliar seu EKS cluster Amazon.
      - `resilience-hub-eks-access-cluster-role-binding`(`ClusterRoleBinding`) — Define um grupo nomeado `resilience-hub-eks-access-group` em seu EKS cluster da Amazon, concedendo a seus usuários as permissões necessárias para executar avaliações de resiliência em. AWS Resilience Hub

      O modelo para conceder acesso de leitura em todos os namespaces ao aplicativo do AWS Resilience Hub é o seguinte:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
    - ""
```

```
  resources:
    - pods
    - replicationcontrollers
    - nodes
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
    - list
```

```
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. Concedendo AWS Resilience Hub acesso para ler namespaces específicos.

Você pode limitar o acesso AWS Resilience Hub a recursos dentro de um conjunto específico de namespaces usando. `RoleBinding` Para isso, você deve criar as seguintes funções:

- `ClusterRole`— AWS Resilience Hub Para acessar os recursos em namespaces específicos dentro de um EKS cluster da Amazon e avaliar sua resiliência, você deve criar as seguintes funções. `ClusterRole`
  - `resilience-hub-eks-access-cluster-role`: especifica as permissões necessárias para avaliar os recursos em namespaces específicos.
  - `resilience-hub-eks-access-global-cluster-role`— Especifica as permissões necessárias para avaliar recursos com escopo de cluster, que não estão associados a um namespace específico, em seus clusters da Amazon. EKS AWS Resilience Hub exige permissões para acessar recursos com escopo de cluster (como nós) em seu EKS cluster da Amazon para avaliar a resiliência do seu aplicativo.

O modelo para criar a função `ClusterRole` é o seguinte:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - pods
      - replicationcontrollers
    verbs:
      - get
      - list
  - apiGroups:
      - apps
    resources:
      - deployments
      - replicasets
    verbs:
      - get
      - list
  - apiGroups:
      - policy
    resources:
      - poddisruptionbudgets
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling.k8s.io
    resources:
      - verticalpodautoscalers
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling
    resources:
      - horizontalpodautoscalers
```

```
    verbs:
      - get
      - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-global-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - nodes
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.sh
    resources:
      - provisioners
      - nodepools
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
      - ec2nodeclasses
    verbs:
      - get
      - list

---
EOF
```

- `RoleBinding`função — Essa função concede as permissões necessárias AWS Resilience Hub para acessar recursos em namespaces específicos. Ou seja, você deve criar uma `RoleBinding` função em cada namespace para permitir o acesso AWS Resilience Hub a recursos dentro de um determinado namespace.

> **Note**
>
> Se você estiver usando `ClusterAutoscaler` para escalonamento automático, você também deve criar `RoleBinding` em `kube-system`. Isso é necessário para avaliar o seu `ClusterAutoscaler`, que faz parte do namespace `kube-system`.
>
> Ao fazer isso, você AWS Resilience Hub concederá as permissões necessárias para avaliar os recursos dentro do `kube-system` namespace enquanto avalia seu cluster da Amazon. EKS

O modelo para criar a função `RoleBinding` é o seguinte:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
  namespace: <namespace>
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

- `ClusterRoleBinding`função — Essa função concede as permissões necessárias AWS Resilience Hub para acessar recursos com escopo de cluster.

  O modelo para criar a função `ClusterRoleBinding` é o seguinte:

```
cat << EOF | kubectl apply -f -
```

```
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-global-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-global-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

3. Atualize o `aws-auth ConfigMap` para mapear o `resilience-hub-eks-access-group` com a IAM função que é usada para acessar o EKS cluster da Amazon.

   Essa etapa cria um mapeamento entre a IAM função usada na etapa 1 e o grupo Kubernetes criado na etapa 2. Esse mapeamento concede permissões às IAM funções para acessar recursos dentro do EKS cluster da Amazon.

   > **Note**
   >
   > - `ROLE-NAME`refere-se à IAM função usada para acessar o EKS cluster da Amazon.
   > - Se seu aplicativo estiver configurado para usar acesso baseado em funções, a função deverá ser a função de invocador ou a função de conta secundária que é passada AWS Resilience Hub durante a criação do aplicativo.
   > - Se seu aplicativo estiver configurado para usar o IAM usuário atual para acessar recursos, ele deverá ser `AwsResilienceHubAssessmentEKSAccessRole` o.
   >
   > - `ACCOUNT-ID`deve ser o ID da AWS conta do EKS cluster da Amazon.

   É possível criar `aws-auth ConfigMap` usando uma das seguintes maneiras:

   - Utilizar o `eksctl`

Use o comando a seguir para atualizar `aws-auth ConfigMap`:

```
eksctl create iamidentitymapping \
 --cluster <cluster-name> \
 --region=<region-code> \
 --arn arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>\
 --group resilience-hub-eks-access-group \
 --username AwsResilienceHubAssessmentEKSAccessRole
```

- Você pode editar manualmente `aws-auth ConfigMap` adicionando os detalhes da IAM função à `mapRoles` seção dos dados `ConfigMap` abaixo. Use o comando a seguir para editar o `aws-auth ConfigMap`.

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  A seção `mapRoles` consiste nos seguintes parâmetros:

  - `rolearn`— O nome do recurso Amazon (ARN) da IAM função a ser adicionada.
    - ARNSintaxe —`arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
  - `username`— O nome de usuário no Kubernetes a ser mapeado para a IAM função (). `AwsResilienceHubAssessmentEKSAccessRole`
  - `groups`: os nomes dos grupos devem corresponder aos nomes dos grupos criados na Etapa 2 (`resilience-hub-eks-access-group`).

  > **Note**
  >
  > Se a seção `mapRoles` não existir, você deverá adicioná-la manualmente.

  Use o modelo a seguir para adicionar os detalhes da IAM função à `mapRoles` seção dos dados `ConfigMap` abaixo.

  ```
    - groups:
      - resilience-hub-eks-access-group
      rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
      username: AwsResilienceHubAssessmentEKSAccessRole
  ```

Habilitando AWS Resilience Hub a publicação em seus tópicos do Amazon Simple Notification Service

Esta seção explica como habilitar AWS Resilience Hub a publicação de notificações sobre o aplicativo em seus tópicos do Amazon Simple Notification Service (AmazonSNS). Para enviar notificações para um SNS tópico da Amazon, verifique se você tem o seguinte:

- Um AWS Resilience Hub aplicativo ativo.
- Um SNS tópico existente da Amazon para o qual AWS Resilience Hub você deve enviar notificações. Para obter mais informações sobre a criação de um SNS tópico na Amazon, consulte Criação de um SNS tópico na Amazon.

Para permitir AWS Resilience Hub a publicação de notificações em seu SNS tópico da Amazon, você deve atualizar a política de acesso do SNS tópico da Amazon com o seguinte:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubPublish",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name"
    }
  ]
}
```

> **Note**
>
> Ao publicar mensagens de regiões opcionais para tópicos localizados em regiões que estão habilitadas por padrão, você deve modificar a política de recursos criada para o SNS tópico da Amazon. AWS Resilience Hub Altere o valor da entidade principal de `resiliencehub.amazonaws.com` para `resiliencehub.<opt-in-region>.amazonaws.com`.

Se você estiver usando um SNS tópico da Amazon com criptografia no lado do servidor (SSE), você deve garantir que AWS Resilience Hub tenha o `Decrypt` acesso `GenerateDataKey` e* à chave de SNS criptografia da Amazon.

Para fornecer `Decrypt` e `GenerateDataKey*` acessar AWS Resilience Hub, você deve incluir as seguintes permissões para AWS Key Management Service acessar a política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubDecrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id"
    }
  ]
}
```

Limitar as permissões para incluir ou excluir recomendações AWS Resilience Hub

AWS Resilience Hub permite restringir as permissões para incluir ou excluir recomendações por aplicativo. Você pode restringir as permissões para incluir ou excluir recomendações por aplicativo usando a seguinte política de IAM confiança. Nesta política de IAM confiança, `caller_IAM_role` (associada à sua conta de AWS usuário) é usada na conta atual APIs para solicitar AWS Resilience Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "resiliencehub:BatchUpdateRecommendationStatus",
```

```
      "Resource": "arn:aws:resiliencehub:us-west-2:12345678900:app/0e6237b7-23ba-4103-
adb2-91811326b703"
    }
  ]
}
```

Segurança da infraestrutura em AWS Resilience Hub

Como serviço gerenciado, AWS Resilience Hub é protegido pelos procedimentos AWS globais de segurança de rede descritos no white paper Amazon Web Services: Overview of Security Processes.

Você usa API chamadas AWS publicadas para acessar AWS Resilience Hub pela rede. Os clientes devem oferecer suporte ao Transport Layer Security (TLS) 1.2 ou posterior. Recomendamos TLS 1.3 ou posterior. Os clientes também devem oferecer suporte a pacotes de criptografia com sigilo direto perfeito (), como Ephemeral Diffie-Hellman (PFS) ou Elliptic Curve Ephemeral Diffie-Hellman (). DHE ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Verificações de resiliência para serviços AWS

Este capítulo fornece os detalhes de várias verificações de resiliência realizadas pelos AWS serviços suportados AWS Resilience Hub para garantir que a postura de resiliência dos aplicativos não seja afetada. Essas verificações estimam o objetivo de tempo de recuperação (RTO) e o objetivo do ponto de recuperação (RPO) em relação aos valores definidos na política de resiliência para cada componente do aplicativo (AppComponent). As avaliações abrangem diferentes tipos de interrupções, ou seja, falhas de aplicativos, de infraestrutura, interrupções de AZ e falhas regionais. No entanto, para executar essas verificações, você deve fornecer IAM permissões relevantes AWS Resilience Hub para permitir que ele acesse seus recursos. Para saber mais sobre as IAM permissões necessárias para permitir o acesso AWS Resilience Hub aos recursos e a realização das verificações de resiliência neste capítulo, consulteAWS políticas gerenciadas para AWS Resilience Hub.

AWS serviços

- Amazon Elastic File System
- Amazon Relational Database Service e Amazon Aurora
- Amazon Simple Storage Service
- Amazon DynamoDB
- Amazon Elastic Compute Cloud
- Amazon EBS
- AWS Lambda
- Amazon Elastic Kubernetes Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Elastic Container Service
- Elastic Load Balancing
- Amazon API Gateway
- Amazon DocumentDB
- NATGateway
- Amazon Route 53
- Controlador de recuperação de aplicativos Amazon (ARC)

- Servidor FSx de arquivos Amazon para Windows
- AWS Step Functions

Amazon Elastic File System

Esta seção lista todas as verificações e recomendações de resiliência que são específicas do Amazon Elastic File System.

Para obter mais informações sobre o Amazon Elastic File System, consulte a documentação do Amazon Elastic File System.

Tipo de sistema de arquivos

AWS Resilience Hub verifica o tipo de sistema de arquivos: regional ou de uma zona. O tipo de sistema de arquivos afeta sua resiliência no caso de interrupções na infraestrutura ou no AZ. Para obter mais informações sobre os tipos de sistemas de arquivos, consulte Disponibilidade e durabilidade dos sistemas de arquivos da Amazon EFS.

Backup do sistema de arquivos

AWS Resilience Hub verifica se um AWS Backup plano está definido para o sistema de arquivos implantado. Além disso, ele verifica se a opção de `Cross-Region` backup está ativada, garantindo cobertura para interrupções em nível regional, se exigido pela política do cliente.

Replicação de dados

AWS Resilience Hub verifica se uma replicação de EFS dados na região ou entre regiões da Amazon está definida para o sistema de arquivos implantado. A replicação de EFS dados da Amazon ajuda a melhorar as estimativas RTO e estimativas RPO nos níveis de aplicativo, infraestrutura, AZ e região. Além disso, AWS Resilience Hub verifica se ele está combinado com uma região interna AWS Backup para permitir a resiliência do sistema de arquivos em caso de interrupção do aplicativo.

Amazon Relational Database Service e Amazon Aurora

Esta seção lista todas as verificações e recomendações de resiliência específicas para o Amazon Relational Database Service e o Amazon Aurora.

Para obter mais informações sobre o Amazon Relational Database Service e o Amazon Aurora, consulte a documentação do Amazon Relational Database Service.

Implantação Single-AZ

AWS Resilience Hub verifica se o banco de dados está implantado como uma única instância e, se determinado, indica que não oferece suporte à instância secundária e à réplica de leitura.

Multi-AZ deployment (Implantação multi-AZ)

AWS Resilience Hub verifica se o banco de dados está implantado com instância secundária ou réplicas de leitura. Se o banco de dados for implantado com réplica de leitura, AWS Resilience Hub valida se ele está implantado em uma AZ diferente para permitir o failover no caso de uma interrupção no AZ.

Backup

AWS Resilience Hub verifica se os seguintes recursos de backup são aplicados em uma instância de banco de dados implantada.

- AWS Backup plano com opção de backup automático
- AWS Backup plano com cópia de backup entre regiões, se exigido pela política do cliente
- Instantâneos manuais para sistemas de backup de terceiros

Failover entre regiões

AWS Resilience Hub verificações RTO e RPO metas definidas na política de resiliência para se recuperar da disrupção regional. Além disso, AWS Resilience Hub pode identificar as seguintes arquiteturas entre regiões para cobrir interrupções regionais:

- Um backup na região com uma cópia de um instantâneo entre regiões
- Uma réplica de leitura em outra região
- Um banco de dados global Amazon Aurora com um cluster secundário em outra região
- Um banco de dados global Amazon Aurora com um cluster secundário sem cabeçalho em outra região

Failover mais rápido na região

AWS Resilience Hub verificações RTO e RPO metas definidas na política de resiliência durante interrupções na infraestrutura ou no AZ. Além disso, AWS Resilience Hub pode identificar as seguintes arquiteturas na região para cobrir interrupções em aplicativos, infraestrutura e AZ:

- Um backup na região
- Uma réplica de leitura em uma AZ diferente
- Um cluster Aurora com uma réplica de leitura em outra AZ
- Uma instância Multi-AZ do Amazon Relational Database Service (Amazon) RDS
- Um cluster Amazon RDS Multi-AZ
- Uma única instância da Amazon RDS com uma réplica de leitura em outra AZ

Amazon Simple Storage Service

Esta seção lista todas as verificações e recomendações de resiliência específicas para o Amazon Simple Storage Service (Amazon S3).

Para obter mais informações sobre o Amazon S3, consulte a documentação do Amazon S3.

Versionamento

AWS Resilience Hub verifica se um bucket do Amazon S3 está configurado com o versionamento ativado.

Backup programado

AWS Resilience Hub verifica se um AWS Backup plano está definido para o bucket implantado do Amazon Simple Storage Service (Amazon S3). Além disso, ele também verifica se a opção de backup entre regiões está ativada se sua política exigir cobertura para interrupções em nível regional.

oint-in-time Recuperação de P

Replicação de dados

AWS Resilience Hub se uma replicação na mesma região (SRR) e uma replicação entre regiões (CRR) forem definidas para o bucket Amazon S3 implantado.

A replicação de dados do Amazon S3 melhora a carga de trabalho estimada RTO e a carga de trabalho estimada RPO em nível de aplicativo, infraestrutura, AZ e região. Além disso, ele também protege contra a exclusão física do objeto, pois a exclusão de uma versão do objeto não é replicada para o bucket de destino do Amazon S3. Além disso, com base nas RTO metas definidas em sua política de resiliência, AWS Resilience Hub verifica se o Amazon S3 Replication Time Control (RTCS3) deve estar ativado ou não. Esse recurso faturável replica 99,99% dos objetos do bucket de origem em 15 minutos.

- AWS Backup plano com opção de backup automático
- AWS Backup plano com cópia de backup entre regiões, se exigido pela política do cliente
- Instantâneos manuais para sistemas de backup de terceiros

Amazon DynamoDB

Esta seção lista todas as verificações e recomendações de resiliência específicas para o Amazon DynamoDB.

Para obter mais informações sobre o Amazon DynamoDB, consulte a documentação do Amazon DynamoDB.

Backup programado

AWS Resilience Hub verifica se um backup já está definido para a tabela implantada. Além disso, ele também verifica se o backup entre regiões deve ser configurado para sua política, caso exija cobertura para interrupções em nível regional.

oint-in-time Recuperação de P

AWS Resilience Hub verifica se point-in-time recovery (PITR) é necessário de acordo com a RPO meta da sua política de resiliência. No entanto, o backup entre regiões não é suportado paraPITR. Portanto, você usa um AWS Backup plano agendado existente com a opção de backup entre regiões ativada ou cria um novo.

Tabela global

Amazon Elastic Compute Cloud

Esta seção lista todas as verificações e recomendações de resiliência que são específicas para o Amazon Elastic Compute Cloud.

Para obter mais informações sobre o Amazon Elastic Compute Cloud, consulte a documentação do Amazon Elastic Compute Cloud.

Instância com estado

AWS Resilience Hub identifica uma EC2 instância da Amazon como uma instância com estado se um dos seguintes critérios for atendido:

- Se o `DeleteOnTermination` atributo for definido como false para pelo menos um volume do Amazon Elastic Block Store (AmazonEBS) anexado a essa instância.
- Se o Amazon Data Lifecycle Manager ou um AWS Backup plano estiver vinculado à EC2 instância da Amazon ou a pelo menos um volume da Amazon. EBS
- AWS Elastic Disaster Recovery É usado para replicar seus volumes de armazenamento de EC2 instâncias da Amazon.

> **Note**
>
> Se uma EC2 instância da Amazon não atender a nenhum dos critérios acima, AWS Resilience Hub trate-a como uma EC2 instância da Amazon sem estado.

Grupos do Auto Scaling

AWS Resilience Hub verifica se há um grupo de EC2 instâncias sem estado da Amazon. Se descoberto, é recomendável orquestrar o mesmo usando grupos de Auto Scaling ASG () com configuração Multi-AZ.

Se um existente ASG for identificado, ARH verificará se ele está configurado em várias zonas de disponibilidade. Se também ASG for definido usando apenas EC2 instâncias spot da Amazon, é recomendável aumentar sua capacidade com EC2 instâncias Amazon sob demanda para melhorar a resiliência

quando as EC2 instâncias spot da Amazon não estão disponíveis.

EC2Frota da Amazon

AWS Resilience Hub identifica a Amazon EC2 Fleet e verifica se ela está definida como implantação Multi-AZ e também se usa somente instâncias spot da AmazonEC2.

Definir uma EC2 frota da Amazon como implantação Multi-AZ melhorará sua resiliência no caso de uma interrupção no AZ.

Aumentar uma EC2 frota da Amazon com instâncias sob demanda melhorará sua resiliência quando as instâncias spot não estiverem disponíveis.

Amazon EBS

Esta seção lista todas as verificações e recomendações de resiliência específicas da AmazonEBS.

Para obter mais informações sobre a AmazonEBS, consulte a EBSdocumentação da Amazon.

Backup programado

AWS Resilience Hub verifica se um ou ambos os itens a seguir estão definidos para seus EBS volumes da Amazon.

- Uma regra de backup para um EBS volume específico da Amazon anexado à sua EC2 instância da Amazon.
- Uma regra de backup para criar uma EC2 instância da Amazon EBS baseada AMI na Amazon.
- Instantâneos manuais para sistemas de backup de terceiros.

Além disso, se sua política exigir cobertura para interrupções em nível regional, AWS Resilience Hub verifique se sua regra de backup tem a opção de backup entre regiões ativada.

Backup e replicação de dados

AWS Resilience Hub identifica que um EBS volume da Amazon é considerado um volume com estado se um dos seguintes critérios for atendido:

- Se o `DeleteOnTermination` atributo estiver definido como falso para este EBS volume da Amazon.

- Se o Amazon Data Lifecycle Manager ou um AWS Backup plano estiver associado a esse volume da Amazon EBS ou à EC2 instância da Amazon à qual ele está vinculado.
- AWS Elastic Disaster Recovery É usado para replicar seus volumes de armazenamento de EC2 instâncias da Amazon.

AWS Lambda

Esta seção lista todas as verificações e recomendações de resiliência que são específicas do. AWS Lambda

Para obter mais informações sobre AWS Lambda, consulte a AWS Lambda documentação.

VPCAcesso ao Amazon para clientes

AWS Resilience Hub identifica uma AWS Lambda função conectada ao clienteVPC. AWS Lambda Conectar-se a sub-redes em diferentes locais AZs da Amazon VPC permite resiliência funcional em caso de interrupção do AZ.

Fila de mensagens não entregues

AWS Resilience Hub verifica se uma AWS Lambda função tem uma fila de letras mortas (DLQ) anexada a ela para armazenar solicitações com falha. Anexar uma AWS Lambda função DLQ to permite evitar a perda de dados das solicitações e tentar processar novamente as solicitações com falha em um estágio posterior.

Amazon Elastic Kubernetes Service

Esta seção lista todas as verificações e recomendações de resiliência que são específicas do Amazon Elastic Kubernetes Service (Amazon). EKS

Para obter mais informações sobre a AmazonEKS, consulte a EKSdocumentação da Amazon.

Multi-AZ deployment (Implantação multi-AZ)

AWS Resilience Hub identifica se a implantação do pod está sendo executada em vários nós de trabalho em váriosAZs.

Um EKS cluster adicional da Amazon em outra região é necessário se sua política de resiliência exigir cobertura em caso de interrupção regional. Esse EKS cluster adicional da Amazon também

é verificado para implantações de pods que são distribuídas entre vários nós de trabalho em váriosAZs.

Implantação vs. ReplicaSet

AWS Resilience Hub verifica se você está usando objetos ReplicaSets de pod em vez de implantar. A substituição de ReplicaSets nossos objetos de pod pela implantação simplifica as atualizações do pod para uma nova versão do software e inclui outros recursos úteis.

Manutenção de implantação

AWS Resilience Hub verifica se as seguintes melhores práticas são usadas para implantação:

- Usando o Pod Disruption Budget (PDB) — O uso PDB possibilita melhorar a disponibilidade definindo um limite para o número de pods na carga de trabalho que podem ser interrompidos a qualquer momento.
- Substituição de grupos de nós autogerenciados por grupos de nós EKS gerenciados pela Amazon — Essa substituição simplifica as atualizações de imagens dos nós de trabalho durante a manutenção.
- Suporte a solicitações dinâmicas CPU e de memória por implantação — Essas solicitações ajudam o Kubernetes a selecionar um nó que atenda às necessidades de um pod.
- Configuração de sondas de atividade e prontidão para todos os contêineres — A configuração de sondas de atividade ajuda a melhorar a resiliência ao reiniciar os pods não funcionais. A configuração das sondas de prontidão possibilita melhorar a disponibilidade desviando o tráfego dos pods ocupados.
- Configurando Karpenter, Cluster Autoscaler ou — AWS Fargate Essas configurações permitem que a infraestrutura do EKS cluster da Amazon cresça e atenda às demandas de carga de trabalho.
- Configuração do Horizontal Pod Autoscaler — Essa configuração ajuda o EKS cluster da Amazon a escalar automaticamente a carga de trabalho para atender à demanda de processamento de solicitações.

Amazon Simple Notification Service

Esta seção lista todas as verificações e recomendações de resiliência que são específicas do Amazon Simple Notification Service (AmazonSNS).

Para obter mais informações sobre a AmazonSNS, consulte a SNSdocumentação da Amazon.

Assinaturas de tópicos

AWS Resilience Hub verifica se o SNS tópico da Amazon tem pelo menos uma assinatura anexada para garantir que as mensagens recebidas não sejam perdidas.

Amazon Simple Queue Service

Esta seção lista todas as verificações e recomendações de resiliência que são específicas do Amazon Simple Queue Service (AmazonSQS).

Para obter mais informações sobre a AmazonSQS, consulte a SQSdocumentação da Amazon.

Fila de mensagens não entregues

AWS Resilience Hub verifica se a SQS fila da Amazon tem uma DLQ associada a ela para lidar com mensagens que não podem ser entregues aos assinantes com sucesso.

Amazon Elastic Container Service

Esta seção lista todas as verificações e recomendações de resiliência que são específicas do Amazon Elastic Container Service (AmazonECS).

Para obter mais informações sobre a AmazonECS, consulte a ECSdocumentação da Amazon.

Multi-AZ deployment (Implantação multi-AZ)

AWS Resilience Hub verifica se ECS as tarefas ou serviços da Amazon estão sendo executados em vários tipos AZs com base na Amazon EC2 ou nos tipos de AWS Fargate lançamento. Um ECS cluster adicional da Amazon em outra região é necessário se sua apólice precisar de cobertura para interrupções regionais. O cluster adicional também é verificado quanto à execução de tarefas ou serviços em váriosAZs.

Elastic Load Balancing

Esta seção lista todas as verificações e recomendações de resiliência que são específicas do Elastic Load Balancing.

Para obter mais informações sobre o Elastic Load Balancing, consulte a documentação do Elastic Load Balancing.

Multi-AZ deployment (Implantação multi-AZ)

AWS Resilience Hub verifica se o Elastic Load Balancing está sendo executado em vários. AZs

Um Elastic Load Balancing adicional em uma região diferente é necessário se sua apólice precisar de cobertura para interrupções regionais. O Elastic Load Balancing adicional, localizado em uma região diferente, também é verificado para sua implantação em várias. AZs

Amazon API Gateway

Esta seção lista todas as verificações e recomendações de resiliência que são específicas do Amazon API Gateway.

Para obter mais informações sobre o Amazon API Gateway, consulte a documentação do Amazon API Gateway.

Implantação entre regiões

Se sua política precisar considerar uma interrupção regional, AWS Resilience Hub verificará se há uma implantação adicional do API recurso Amazon API Gateway em uma região diferente.

Implantação privada API de Multi-AZ

AWS Resilience Hub verifica se você API está definido como privado no Amazon API Gateway. O privado APIs deve receber tráfego por meio do endpoint de VPC interface da Amazon, que é implantado em vários. AZs

Amazon DocumentDB

Esta seção lista todas as verificações e recomendações específicas do Amazon DocumentDB.

Para obter mais informações sobre o Amazon DocumentDB, consulte a documentação do Amazon DocumentDB.

Multi-AZ deployment (Implantação multi-AZ)

AWS Resilience Hub verifica se o cluster Amazon DocumentDB está implantado em vários. AZs Um cluster secundário adicional do Amazon DocumentDB é necessário em uma região diferente se sua

política exigir cobertura para interrupções regionais. O cluster adicional do Amazon DocumentDB, localizado em uma região diferente, também é verificado quanto à sua execução em várias. AZs

Cluster elástico e implantação Multi-AZ

AWS Resilience Hub verifica se os fragmentos de cluster elásticos do Amazon DocumentDB estão usando réplicas de leitura implantadas em diferentes. AZs

Cluster elástico e instantâneos manuais

AWS Resilience Hub verifica se os snapshots manuais são criados regularmente para um cluster elástico do Amazon DocumentDB. Os instantâneos manuais permitem maior persistência e oferecem flexibilidade na configuração da frequência dos instantâneos de acordo com as necessidades da sua empresa.

NATGateway

Esta seção lista todas as verificações e recomendações específicas do NAT Gateway. Para obter mais informações sobre NAT gateways, consulte NATGateways.

Multi-AZ deployment (Implantação multi-AZ)

AWS Resilience Hub verifica se o NAT Gateway está implantado em váriosAZs.

Uma implantação adicional do NAT Gateway é necessária em uma região diferente se sua apólice exigir cobertura para interrupções regionais. O NAT Gateway adicional, localizado em uma região diferente, também é verificado para sua implantação em váriasAZs.

Amazon Route 53

Esta seção lista todas as verificações e recomendações específicas do Amazon Route 53.

Para obter mais informações sobre o Amazon Route 53, consulte a documentação do Amazon Route 53.

Multi-AZ deployment (Implantação multi-AZ)

AWS Resilience Hub verifica se o registro da zona hospedada do Amazon Route 53 está definido com vários destinos na mesma região e se esses alvos estão implantados em váriosAZs. Se sua política exigir cobertura para interrupções regionais, AWS Resilience Hub verifique se o registro da

zona hospedada do Amazon Route 53 está definido em várias regiões com vários alvos por região e se esses alvos estão implantados em vários. AZs

Controlador de recuperação de aplicativos Amazon (ARC)

Esta seção lista todas as verificações e recomendações específicas do Amazon Application Recovery Controller (ARC) (ARC).

Para obter mais informações sobreARC, consulte a ARCdocumentação.

Multi-AZ deployment (Implantação multi-AZ)

AWS Resilience Hub verifica se recursos semelhantes estão implantados em várias regiões e recomenda, como melhor prática, definir verificações de ARC prontidão para aumentar sua disponibilidade e prontidão no caso de uma interrupção regional. Você será notificado de que incorrerá em cobranças adicionais por hora.

Servidor FSx de arquivos Amazon para Windows

Esta seção lista todas as verificações e recomendações específicas do Amazon FSx para Windows File Server. Para obter mais informações sobre o Amazon FSx para Windows File Server, consulte a documentação do Amazon FSx para Windows File Server.

Tipo de sistema de arquivos

AWS Resilience Hub verifica o tipo de sistema de arquivos: ou. `Regional` `One Zone` O tipo de sistema de arquivos afeta sua resiliência no caso de interrupções na infraestrutura ou no AZ. Para obter mais informações sobre os tipos de sistemas de arquivos, consulte Amazon. EFS

Backup do sistema de arquivos

AWS Resilience Hub verifica se um AWS Backup está definido para o sistema de arquivos implantado. Além disso, ele também verifica se a `cross-Region backup` opção está ativada se sua apólice exige cobertura para interrupções em nível regional.

Replicação de dados

AWS Resilience Hub verifica se uma tarefa de replicação de AWS DataSync dados agendada na região ou entre regiões está definida para o sistema de arquivos implantado.

AWS DataSync a tarefa programada de replicação de dados pode melhorar a carga de trabalho estimada RTO e a carga de trabalho estimada RPO nos níveis de infraestrutura, AZ e região. Além disso, ele pode ser combinado com uma região interna AWS Backup para recuperação em caso de interrupção do aplicativo.

AWS Step Functions

Esta seção lista todas as verificações e recomendações específicas do AWS Step Functions.

Para obter mais informações sobre AWS Step Functions, consulte a AWS Step Functions documentação.

Controle de versão e alias

AWS Resilience Hub verifica se o AWS Step Functions fluxo de trabalho usa controle de versão e alias para melhorar o tempo de reimplantação.

Implantação entre regiões

AWS Resilience Hub verifica se o AWS Step Functions fluxo de trabalho do mesmo tipo de fluxo de trabalho está implantado em uma região diferente para se recuperar no caso de uma interrupção regional.

Como trabalhar com outros serviços do

Esta seção descreve AWS os serviços que interagem com AWS Resilience Hub.

Tópicos

- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- AWS Trusted Advisor

AWS CloudFormation

O AWS Resilience Hub está integrado ao AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus recursos da AWS para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os recursos do AWS desejados (como AWS: :ResilienceHub: :ResiliencyPolicy e AWS: :ResilienceHub: ::App) e o AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar o AWS CloudFormation, você poderá reutilizar seu modelo para configurar seus recursos do AWS Resilience Hub de forma repetida e consistente. Descreva seus recursos uma vez e, depois, provisione os mesmos recursos repetidamente em várias contas e regiões da AWS.

Modelos do AWS Resilience Hub e do AWS CloudFormation

Para provisionar e configurar recursos para o AWS Resilience Hub e serviços relacionados, você deve entender os Modelos do AWS CloudFormation. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar nas suas pilhas do AWS CloudFormation. Se você não estiver familiarizado com JSON ou YAML, poderá usar o AWS CloudFormation Designer para ajudá-lo a começar a usar os modelos do AWS CloudFormation. Para obter mais informações, consulte O que é o AWS CloudFormation Designer no Manual do usuário do AWS CloudFormation.

O AWS Resilience Hub oferece suporte à criação de AWS::ResilienceHub:::ResiliencyPolicy and AWS::ResilienceHub:::App no AWS CloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para AWS::ResilienceHub:::ResiliencyPolicy e

AWS::ResilienceHub:::App, consulte a Referência de tipo de recurso do AWS Resilience Hub no Guia do usuário do AWS CloudFormation.

Você pode usar pilhas do AWS CloudFormation para definir aplicativos do AWS Resilience Hub. Uma pilha permite gerenciar recursos relacionados como uma unidade única. Uma pilha pode conter todos os recursos necessários para executar um aplicativo web, como um servidor web ou as regras de rede.

Saiba mais sobre o AWS CloudFormation

Para obter mais informações sobre o AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- Manual do usuário do AWS CloudFormation
- Referência da API do AWS CloudFormation
- Guia do usuário da interface de linha de comando do AWS CloudFormation

AWS CloudTrail

AWS Resilience Hub é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um AWS serviço em AWS Resilience Hub. CloudTrail captura todas as chamadas de API AWS Resilience Hub como eventos. As chamadas capturadas incluem chamadas do AWS Resilience Hub console e chamadas de código para as operações da AWS Resilience Hub API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AWS Resilience Hub 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 AWS Resilience Hub, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

AWS Systems Manager

AWS Resilience Hub trabalha com o Systems Manager para automatizar as etapas de seus SOPs, fornecendo vários documentos SSM que você pode usar como base para esses SOPs.

AWS Resilience Hub fornece AWS CloudFormation modelos que contêm as funções do IAM necessárias para executar diferentes documentos do Systems Manager, uma função por documento com as permissões necessárias para o documento específico. Depois de criar uma pilha com o AWS CloudFormation modelo, ele configurará as funções do IAM e salvará os metadados no parâmetro Systems Manager para que o documento de automação do Systems Manager seja executado em diferentes procedimentos de recuperação.

Para obter mais informações sobre como usar os SOPs, consulte Gerenciando procedimentos operacionais padrão.

AWS Trusted Advisor

AWS Trusted Advisor é um local centralizado de recomendações de AWS melhores práticas que ajuda você a identificar, priorizar e otimizar sua implantação em. AWS AWS Trusted Advisor inspeciona seu AWS ambiente e, em seguida, faz recomendações por meio de verificações quando existem oportunidades para economizar dinheiro, melhorar a disponibilidade e o desempenho do sistema ou ajudar a fechar lacunas de segurança. Essas verificações são divididas em várias categorias com base em sua finalidade. Para obter mais informações sobre diferentes categorias de check-in AWS Trusted Advisor, consulte o Guia AWS Supportdo usuário.

AWS Trusted Advisor fornece várias recomendações de resiliência de alto nível por meio de verificações de resiliência para cada aplicativo na AWS Resilience Hub categoria de tolerância a falhas. A categoria de tolerância a falhas lista todas as verificações que testam seus aplicativos para determinar sua resiliência e confiabilidade. Essas verificações alertam você quando há AppComponent falhas e violações de políticas que podem causar riscos de resiliência e afetar a disponibilidade do aplicativo para a continuidade dos negócios. Ele também fornece recomendações de resiliência que aumentarão as chances de reduzir esses riscos na seção Ação Recomendada, que precisa ser abordada em AWS Resilience Hub. Para obter mais informações sobre as recomendações para cada aplicativo no AWS Trusted Advisor, recomendamos que você veja as recomendações detalhadas fornecidas no AWS Resilience Hub.

AWS Trusted Advisor fornece as seguintes verificações para cada aplicativo em AWS Resilience Hub:

- AWS Resilience Hub pontuações de resiliência de aplicativos — verifica a pontuação de resiliência de seus aplicativos a partir da avaliação mais recente AWS Resilience Hub e alerta se suas pontuações de resiliência estiverem abaixo de um valor específico.

  Critérios de alerta

- Verde — Indica que seu aplicativo tem uma pontuação de resiliência de 70 ou mais.
- Amarelo — Indica que seu aplicativo tem uma pontuação de resiliência entre 40 e 69.
- Vermelho — Indica que seu aplicativo tem uma pontuação de resiliência menor que 40.

Ação recomendada

Para melhorar a postura de resiliência e obter a melhor pontuação de resiliência possível para seu aplicativo, execute uma avaliação com a versão atualizada mais recentemente dos recursos do aplicativo e, se aplicável, implemente as recomendações operacionais sugeridas. Para obter mais informações sobre como executar, revisar e implementar avaliações, revisar e incluir/excluir recomendações operacionais e implementá-las, consulte os tópicos a seguir:

- the section called “Executar avaliações de resiliência”
- the section called “Analisar relatórios de avaliações”
- the section called “Analisar recomendações de resiliência”
- the section called “Incluir ou excluir recomendações operacionais”

- AWS Resilience Hub violação da política de aplicativos — verifica se os AWS Resilience Hub aplicativos atendem às metas de RTO e RPO que você definiu para um aplicativo e alerta se o aplicativo não atingir as metas de RTO e RPO.

  Critérios de alerta

  - Verde — Indica que o aplicativo tem uma política e que a carga de trabalho estimada RTO e a carga de trabalho estimada RPO atendem às metas de RTO e RPO.
  - Amarelo — Indica que o aplicativo tem uma política e não foi avaliado.
  - Vermelho — Indica que o aplicativo tem uma política e que o RTO da carga de trabalho estimada e o RPO da carga de trabalho estimada não atendem às metas de RTO e RPO.

  Ação recomendada

  Para garantir que a RTO da carga de trabalho estimada e o RPO da carga de trabalho estimada do seu aplicativo ainda atendam às metas definidas de RTO e RPO, execute avaliações regularmente com a versão atualizada mais recentemente dos recursos do seu aplicativo. Além disso, se você quiser garantir que a política de resiliência do seu aplicativo não seja violada, recomendamos que você revise o relatório de avaliação e implemente as recomendações de resiliência sugeridas. Para obter mais informações sobre como AWS Resilience Hub permitir a execução diária de avaliações em seu nome, a execução de avaliações, a revisão das recomendações de resiliência e a implementação das mesmas, consulte os tópicos a seguir:

- the section called “Editar recursos de aplicativo”(AWS Resilience Hub Para permitir a execução diária de avaliações em seu nome, conclua as etapas em Para editar as configurações de notificação de deriva do seu procedimento de inscrição para marcar a caixa de seleção Avaliar automaticamente diariamente.)
- the section called “Executar avaliações de resiliência”
- the section called “Analisar relatórios de avaliações”
- the section called “Analisar recomendações de resiliência”
- the section called “Incluir ou excluir recomendações operacionais”

- AWS Resilience Hub idade de avaliação de aplicativos — Verifica a última vez desde que você executou uma avaliação para cada um de seus aplicativos em AWS Resilience Hub. Emite um alerta se você não tiver executado uma avaliação para o número especificado de dias.

  Critérios de alerta

  - Verde — Indica que você realizou uma avaliação para sua inscrição nos últimos 30 dias.
  - Amarelo — Indica que você não realizou uma avaliação para sua inscrição nos últimos 30 dias.

  Ação recomendada

  Faça avaliações regularmente para gerenciar e melhorar a postura de resiliência de seus aplicativos no. AWS Se quiser AWS Resilience Hub avaliar seu aplicativo diariamente em seu nome, você pode habilitá-lo marcando a caixa de seleção Avaliar automaticamente este aplicativo diariamente na notificação de AWS Resilience Hub desvio. Para marcar a caixa de seleção Avaliar automaticamente este aplicativo diariamente, preencha o procedimento Para editar a notificação de desvio do seu aplicativo em???.

  > **Note**
  >
  > Essa verificação determina a idade de avaliação apenas das inscrições que foram avaliadas pelo menos uma vez. AWS Resilience Hub

- AWS Resilience Hub verificação do componente do aplicativo — Verifica se um componente do aplicativo (AppComponent) em seu aplicativo é irrecuperável. Ou seja, se isso AppComponent não se recuperar no caso de um evento de interrupção, você poderá experimentar perda de dados desconhecida e tempo de inatividade do sistema. Se o critério de alerta estiver definido como vermelho, isso indica que AppComponent é irrecuperável.

  Ação recomendada

Para garantir que seu AppComponent seja recuperável, analise e implemente as recomendações de resiliência e, em seguida, execute uma nova avaliação. Para obter mais informações sobre a revisão das recomendações de resiliência, consulte. the section called “Analisar recomendações de resiliência”

Para obter mais informações sobre o uso AWS Trusted Advisor, consulte o Guia AWS Support do usuário.

Histórico de documentos para o Guia AWS Resilience Hub do usuário

A tabela a seguir descreve a documentação desta versão do AWS Resilience Hub.

- APIversão: mais recente
- Última atualização da documentação: 01 de agosto de 2024

Alteração	Descrição	Data
AWS Resilience Hub apresenta recomendações de agrupamento	AWS Resilience Hub introduz uma nova opção de agrupamento inteligente para agrupar recursos em componentes de aplicativos (AppComponents) enquanto integra seus aplicativos. Ao realizar avaliações de resiliênc ia AWS Resilience Hub, é importante que seus recursos sejam agrupados com precisão e sejam apropriados AppComponents para receber recomendações otimizadas e acionáveis. Essa opção é ideal para aplicativos complexos ou entre regiões para reduzir o tempo necessário para integrar seus aplicativos e complementa o fluxo de trabalho de integração de aplicativos existente que está disponível atualmente.	1º de agosto de 2024

	Para obter mais informações, consulte os tópicos a seguir. • the section called “Gerenciando componentes do aplicativo” • the section called “AWS Resilience Hub recomendações de agrupamento de recursos”	
AWS Resilience Hub introduz um novo widget de resumo da avaliação	AWS Resilience Hub apresenta um novo widget de resumo da avaliação que usa os recursos de IA generativa do Amazon Bedrock para transformar dados complexos de resiliência em insights altamente acionáveis. Esses resumos de avaliação extraem as descobertas críticas, priorizam os riscos e recomendam etapas para melhorar a resiliência. Ao se concentrar nos elementos mais impactantes, você pode entender as avaliações com muito mais facilidade, o que ajuda você com informações de alto impacto que se concentram nos elementos mais críticos de sua postura de resiliência. Para obter mais informações, consulte the section called “Resumo da avaliação”.	1º de agosto de 2024

AWS Resilience Hub estende o suporte ao Amazon DocumentDB	Essa AWS Resilience Hub política permite que você conceda `Describe` permissões para acessar recursos e configurações no Amazon DocumentDB, no Elastic Load Balancing AWS Lambda e durante a execução de avaliações. Para obter mais informações sobre a política AWS gerenciada, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”.	1º de agosto de 2024

AWS Resilience Hub expande os recursos de detecção de desvios de resiliência de aplicativos	AWS Resilience Hub expandiu seus recursos de detecção de deriva introduzindo um novo tipo de detecção de deriva — desvio de recursos de aplicativos. Esse aprimoramento detecta alterações, como adição ou exclusão de recursos nas fontes de entrada do aplicativo. Você pode ativar os serviços de avaliação AWS Resilience Hub programada e notificação de desvio e ser notificado sempre que ocorrer um desvio. A avaliação de resiliência mais recente identifica os desvios e apresenta ações de remediação para que o aplicativo volte à conformidade com sua política de resiliência. Para obter mais informações, consulte os tópicos a seguir. • the section called “Detecção de desvios” • the section called “Etapa 5: configurar a avaliação programada e a notificação de deriva”	8 de maio de 2024

AWS Trusted Advisor aprimoramentos	AWS Resilience Hub expandiu o suporte AWS Trusted Advisor ao adicionar uma verificação para identificar componentes de aplicativos irrecuperáveis ()AppComponents. Para obter mais informações, consulte the section called “AWS Trusted Advisor”.	28 de março de 2024
AWS Resilience Hub estende o suporte para alarmes recomendados	AWS Resilience Hub atualizou o arquivo de `README.md` modelo com valores que permitem criar alarmes recomendados por AWS Resilience Hub dentro AWS (como a Amazon CloudWatch) ou por fora AWS. Para obter mais informações, consulte the section called “Gerenciar alarmes”.	26 de março de 2024

AWS Resilience Hub estende o suporte ao Amazon FSx para Windows File Server	AWS Resilience Hub estende o suporte de avaliação para os recursos do Amazon FSx for Windows File Server enquanto avalia a resiliência do seu aplicativo. Para aplicativos que usam o Amazon FSx for Windows File Server, AWS Resilience Hub fornece um novo conjunto de recomenda ções de resiliência, abrangend o implantações de Zona de Disponibilidade (AZ) e Multi-AZ, planos de backup e replicação de dados. AWS Resilience Hub oferece suporte ao Amazon FSx para Windows File Server, incluindo a dependência do sistema de arquivos no Microsoft Active Directory, para implantações na região e entre regiões. Para obter mais informações, consulte os tópicos a seguir. • the section called “ AWS Resilience Hub Recursos suportados” • the section called “AWSResilienceHubA sssessmentExecutionPolicy” • the section called “Agrupand o recursos em um componente de aplicativo”	26 de março de 2024

AWS Resilience Hub fornece informações adicionais sobre a pontuação de resiliência	AWS Resilience Hub atualizou a experiência do usuário do Resiliency Score para ajudá-lo a navegar e entender facilmente as ações necessári as para melhorar a postura de resiliência de seus aplicativos. Para obter mais informações, consulte the section called “Entender as pontuações de resiliência”.	9 de novembro de 2023
AWS Resilience Hub amplia o suporte para aplicativos que incluem recursos do Amazon Elastic Kubernetes Service (Amazon) EKS	AWS Resilience Hub estende o suporte para aplicativos que incluem EKS recursos da Amazon para incluir novas recomendações operacionais. Ao executar uma avaliação que inclui recursos dos EKS clusters da Amazon, agora recomendaremos a execução de testes e alarmes para ajudar a melhorar a postura de resiliência dos aplicativos. Para obter mais informações, consulte the section called “Gerenciando experimentos do Amazon Fault Injection Service”.	9 de novembro de 2023

AWS Resilience Hub fornece informações adicionais no nível do aplicativo	AWS Resilience Hub fornece informações adicionais no nível do aplicativo sobre a carga de trabalho estimada RTO e a carga de trabalho RPO estimada. Essas informações adicionais indicam a carga de trabalho estimada máxima possível RTO e a carga de trabalho estimada RPO de seu aplicativ o a partir da última avaliação bem-sucedida. Esse valor é a carga de trabalho máxima estimada RTO e a carga de trabalho estimada RPO de todos os tipos de interrupção. Para obter mais informações, consulte the section called “Gerenciar aplicações”.	30 de outubro de 2023

AWS Resilience Hub amplia o suporte de avaliação para AWS Step Functions recursos	AWS Resilience Hub amplia o suporte de avaliação de AWS Step Functions recursos enquanto avalia a resiliênc ia do seu aplicativo. AWS Resilience Hub analisa a AWS Step Functions configuração, incluindo o tipo de máquina de estado (fluxos de trabalho Standard ou Express). Além disso, também AWS Resilienc e Hub fornecerá recomenda ções que ajudarão você a atingir os objetivos estimados de tempo de recuperação da carga de trabalho (RTO) e os objetivos estimados de ponto de recuperação da carga de trabalho (RPO). Para avaliar os aplicativos, incluindo AWS Step Functions os recursos, você deve configura r as permissões necessári as, usando a política AWS gerenciada ou adicionando manualmente a permissão específica AWS Resilience Hub para permitir a leitura da AWS Step Functions configur ação. Para obter mais informaçõ es sobre as permissões associadas, consulte the section called “AWSResil	30 de outubro de 2023

ienceHubAsssessmen
tExecutionPolicy”.

AWS Resilience Hub permite excluir recomendações operacionais	AWS Resilience Hub adiciona a capacidade de excluir recomendações operacionais, incluindo alarmes, procedimentos operacionais padrão (SOPs) e testes do Amazon Fault Injection Service (AWS FIS). Ao executar uma avaliação AWS Resilience Hub, você recebe tempos de recuperação estimados e recomendações sobre formas de aumentar a resiliência do aplicativo que foi avaliado. Usando o fluxo de trabalho de exclusão de recomendações, agora você poderá excluir alarmes recomendados e AWS FIS testes que não são relevantes para eles. SOPs O fluxo de trabalho de exclusão é benéfico se você estiver usando uma plataforma fora da sugerida ou se já tiver implementado a recomendação em um método alternativo. Para obter mais informações, consulte os tópicos a seguir. • the section called “Incluir ou excluir recomendações operacionais” • the section called “Limitar as permissões para incluir ou	9 de agosto de 2023

	excluir recomendações do AWS Resilience Hub ”	
Melhorando o design de permissões para AWS Resilience Hub	AWS Resilience Hub apresenta um novo design de permissão para fornecer flexibilidade ao configurar funções AWS Identity and Access Management (IAM) para. AWS Resilience Hub Ele também consolida as permissões em uma única função, com a capacidade de criar nomes de funções personalizados que sejam significativos para você e suas equipes. Uma nova política gerenciada AWS Resilience Hub permitirá que você tenha as permissões apropriadas para os serviços suportados. Se estiver familiarizado com o método atual de definição de permissões, continuar emos oferecendo suporte à configuração manual. Para obter mais informaçõ es sobre a política AWS gerenciada, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”.	2 de agosto de 2023

Detecção de desvios de resiliência de aplicativos com AWS Resilience Hub	AWS Resilience Hub permite que você detecte e compreend a proativamente as ações necessárias para resolver a resiliência do aplicativ o. Permitir que o Amazon Simple Notification Service (AmazonSNS) receba notificações quando o objetivo estimado do tempo de recuperação da carga de trabalho (RTO) ou o objetivo estimado do ponto de recuperação da carga de trabalho (RPO) deixar de atingir a meta para não satisfazer mais os objetivos comerciais da sua organizaç ão. Passar da busca reativa de problemas de resiliência durante a execução manual de uma avaliação para a notificaç ão proativa por meio de SNS tópicos da Amazon permitirá que você antecipe possíveis interrupções mais cedo e forneça mais confiança de que os objetivos de recuperação serão alcançados. Para obter mais informações, consulte os tópicos a seguir. • the section called “Etapa 5: configurar a avaliação programada e a notificação de deriva”	2 de agosto de 2023

- the section called “Editar recursos de aplicativo”

AWS Resilience Hub melhora o suporte ao Amazon Relational Database Service e ao Amazon Aurora	AWS Resilience Hub amplia o suporte de avaliação para o proxy do Amazon Relational Database Service e para as configurações de banco de dados headless e Amazon Aurora DB. Além disso, ao avaliar aplicativos que incluem a AmazonRDS, agora distinguiremos entre diferentes mecanismos de banco de dados para fornecer objetivos de tempo de recuperação de carga de trabalho estimados mais precisos ()RTOs. AWS Resilience Hub também fornecerá ações adicionais para implementar as melhores práticas de resiliência em seu AWS ambiente. As melhores práticas podem incluir insights de desempenho com o DevOps Guru for AmazonRDS, monitoramento aprimorado e automação de implantação azul/verde em mecanismos de banco de dados compatíveis. Para saber mais sobre as permissões necessárias AWS Resilience Hub para incluir recursos de todos os serviços suportados em sua avaliação, consultethe section called “AWSResilienceHubAsssessmentExecutionPolicy”.	2 de agosto de 2023

AWS Resilience Hub amplia o suporte para snapshots do Amazon Elastic Block Store	AWS Resilience Hub estende o suporte de avaliação para o Amazon Elastic Block Store (AmazonEBS) para reconhecer EBS snapshots da Amazon, que são tirados na mesma EBS região da Amazon usando o DirectAPIs. O suporte estendido é adicional ao suporte atual para clientes que usam o Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) ou o Backup. AWS Para obter mais informações, consulte Amazon Elastic Block Store (AmazonEBS).	2 de agosto de 2023

Aprimoramentos do Amazon Elastic Compute Cloud	AWS Resilience Hub expandiu o suporte para o Amazon Elastic Compute Cloud (AmazonEC2). Para aplicativos de tamanhos diferentes, AWS permite que seus clientes que usam EC2 a Amazon selecionem a configuração apropriada para seu caso de uso. AWS Resilience Hub oferece suporte à avaliação nas seguintes EC2 configurações da Amazon: • Instâncias sob demanda. • Backup de instâncias por AWS Backup AWS Elastic Disaster Recovery e. • Support para grupos de auto-scaling com o Amazon Application Recovery Controller ARC () () ARC No futuro, o suporte de avaliação se estenderá para incluir instâncias spot, hosts dedicados, instâncias dedicadas, grupos de posicionamento e frotas. Para obter mais informações, consulte the section called “AWS Resilience Hub referência de permissões de acesso”.	27 de junho de 2023

AWS atualizações de políticas gerenciadas	Foi adicionada uma nova política que fornece acesso a outros AWS serviços para a execução de avaliações. Para obter mais informaçõ es, consulte the section called “AWSResilienceHubA sssessmentExecutionPolicy”.	26 de junho de 2023
Novos alarmes de recomenda ção operacional do Amazon DynamoDB	Para aplicativos que usam o Amazon DynamoDB AWS Resilience Hub , agora fornece um novo conjunto de alarmes que alertam sobre riscos de resiliência para modos de capacidade provisionados e sob demanda e tabelas globais. Para acessar os novos alarmes, talvez seja necessário atualizar a política AWS Identity and Access Management (IAM) da função que você está usando. Para obter mais informaçõ es, consulte the section called “AWS Resilience Hub referência de permissões de acesso”.	2 de maio de 2023

AWS Trusted Advisor aprimoramentos	AWS Resilience Hub expandiu o suporte AWS Trusted Advisor e os aplicativos que usam o Amazon DynamoDB. Ao usar AWS Trusted Advisor com AWS Resilience Hub, agora você pode receber uma notificação quando uma inscrição não tiver sido avaliada nos últimos 30 dias. Essa notificação solicita que você reavalie o aplicativo para entender se há alguma alteração que possa afetar sua resiliência. Para obter mais informaçõ es sobre a verificação da Idade de avaliação do AWS Resilience Hub , consulte the section called “AWS Trusted Advisor”.	2 de maio de 2023

Suporte adicional para o Amazon Simple Storage Service	Além do suporte atual do Amazon Simple Storage Service (Amazon S3), a replicação entre regiões (Amazon S3) e a replicação na mesma região do Amazon S3 (CRR), o controle de versão e o backup agora AWS Resilience Hub avaliarão o Amazon S3 como ponto de acesso multirregional, controle de tempo de replicação do Amazon S3 SRR (Amazon S3) e Configuração de AWS backup e recuperação (). RTC AWS point-in-time PITR Para obter mais informações, consulte os tópicos a seguir. • the section called “AWS Resilience Hub referência de permissões de acesso” • Gerenciar seu armazenamento do Amazon S3	21 de março de 2023

Suporte adicional para o Amazon Elastic Kubernetes Service	AWS Resilience Hub adicionou o EKS cluster da Amazon como um recurso compatível para definir, validar e rastrear a resiliência do aplicativo. Os clientes podem adicionar EKS clusters da Amazon a aplicativos novos ou existentes e receber avaliações e recomendações para melhorar a resiliência. Os clientes podem adicionar recursos de aplicativos usando AWS CloudFormation Terraform e. AWS Resource Groups AppRegistry Além disso, os clientes podem adicionar um ou mais EKS clusters da Amazon diretamen te em uma ou mais regiões com um ou mais namespaces em cada cluster. Isso permite AWS Resilience Hub fornecer avaliações e recomenda ções únicas e interregionais. Além de examinar implantaç ões, réplicas e pods Replicati onControllers, AWS Resilienc e Hub analisará a resiliênc ia geral do cluster. AWS Resilience Hub suporta cargas de trabalho de EKS cluster sem estado da Amazon. Os novos recursos estão disponíveis em todas as	21 de março de 2023

	AWS regiões em que AWS Resilience Hub há suporte. Para obter mais informações, consulte os tópicos a seguir. • the section called “Etapa 2: gerenciar os recursos do seu aplicativo” • the section called “Adicionar EKS clusters” • the section called “AWS Resilience Hub referência de permissões de acesso” • AWS Serviços regionais	
Suporte adicional para o Amazon Elastic File System	Além do suporte atual para o backup do Amazon Elastic File System (AmazonEFS), agora AWS Resilience Hub avaliará a EFS replicação e a configura ção de AZ da Amazon EFS para Amazon. Para obter mais informações, consulte os tópicos a seguir. • the section called “ AWS Resilience Hub Recursos suportados” • O que é o Amazon Elastic File System?	21 de março de 2023

Suporte para fontes de entrada de aplicativos	AWS Resilience Hub agora fornece transparência sobre as fontes do seu aplicativo. Ele ajuda você a adicionar, excluir e reimportar fontes de entrada do seu aplicativo e publicar uma nova versão do aplicativo. Para obter mais informações, consulte the section called “Editar recursos de aplicativo”.	21 de fevereiro de 2023
Suporte para parâmetros de configuração de aplicativo	AWS Resilience Hub agora fornece um mecanismo de entrada para coletar informações adicionais sobre os recursos associados aos seus aplicativos. Com essas informações, AWS Resilienc e Hub obterá uma compreens ão mais profunda de seus recursos e fornecerá melhores recomendações de resiliência. Para obter mais informações, consulte os tópicos a seguir. • the section called “Parâmetr os de configuração do aplicativo” • the section called “Etapa 7: configurar os parâmetros de configuração do aplicativo” • the section called “Atualizar parâmetros de configuração do aplicativo”	21 de fevereiro de 2023

Suporte adicional para o Amazon Elastic Block Store	Além do suporte atual aos volumes do Amazon Elastic Block Store (AmazonEBS), agora AWS Resilience Hub avaliará os EBS snapshots da Amazon pelo Amazon Data Lifecycle Manager e pelo EBS Amazon fast snapshot restore (). FSR Para obter mais informações, consulte os tópicos a seguir. • the section called “AWS Resilience Hub referência de permissões de acesso” • Amazon Elastic Block Store (AmazonEBS)	21 de fevereiro de 2023

Integração com AWS Trusted Advisor	AWS Trusted Advisor os usuários poderão visualizar os aplicativos associados à sua conta que foram avaliados por AWS Resilience Hub. AWS Trusted Advisor mostra a pontuação de resiliênc ia mais recente e fornece um status que indica se a política de resiliência alvo (RTOeRPO) foi cumprida ou não. Sempre que uma avaliação é executada, ela é AWS Resilience Hub atualizad a AWS Trusted Advisor com os resultados mais recentes. AWS Trusted Advisor é um serviço que analisa continuam ente suas AWS contas e fornece recomendações para ajudá-lo a seguir as AWS melhores práticas e as diretrizes da AWS Well-Arch itected. Para obter mais informações, consulte the section called “AWS Trusted Advisor”.	18 de novembro de 2022

Support for Amazon Simple Notification Service (AmazonSNS)	AWS Resilience Hub agora avalia os aplicativos que usam a Amazon SNS analisando a SNS configuração da Amazon, incluindo assinantes, e fornece recomendações para atender aos objetivos estimados de recuperação da carga de trabalho da organização (carga de trabalho estimada RTO e carga de trabalho estimadaRPO) para os aplicativos. SNSA Amazon é um serviço gerenciado que entrega mensagens de editores (produtores) para assinantes (consumidores). Para obter mais informações, consulte os tópicos a seguir. • the section called “ AWS Resilience Hub Recursos suportados” • the section called “Identity and Access Management” • the section called “Agrupando recursos em um componente de aplicativo”	16 de novembro de 2022

Support adicional para Amazon Application Recovery Controller (ARC) (AmazonARC)	AWS Resilience Hub agora avalia a Amazon ARC para Elastic Load Balancing e o Amazon Relational Database Service (RDSAmazon), o que inclui orientação sobre quando ARC a Amazon seria benéfica. Estendendo AWS Resilienc e Hub o suporte de ARC avaliação da Amazon além do AWS Auto Scaling Group AWS ASG () e do Amazon DynamoDB. ARCA Amazon fornece alta disponibilidade para seu aplicativo, permitindo que você transfira rapidamen te todo o aplicativo para uma região de failover. Para obter mais informações, consulte os tópicos a seguir. • the section called “ AWS Resilience Hub Recursos suportados” • the section called “Identity and Access Management”	16 de novembro de 2022

Support adicional para AWS Backup	AWS Resilience Hub agora avalia a Amazon ARC para Elastic Load Balancing e o Amazon Relational Database Service (RDSAmazon), o que inclui orientação sobre quando ARC a Amazon seria benéfica. Estendendo AWS Resilienc e Hub o suporte de ARC avaliação da Amazon além do AWS Auto Scaling Group AWS ASG () e do Amazon DynamoDB. ARCA Amazon fornece alta disponibilidade para seu aplicativo, permitindo que você transfira rapidamen te todo o aplicativo para uma região de failover. Para obter mais informações, consulte os tópicos a seguir. • the section called “ AWS Resilience Hub Recursos suportados” • the section called “Identity and Access Management”	16 de novembro de 2022
Conteúdo atualizado: novos recursos do componente de aplicativo foram adicionados	O Route53 e o AWS Backup foram adicionados à lista de recursos de componentes de aplicativos suportados na seção de AppComponent agrupamento.	1° de julho de 2022

Novo conteúdo: conceito de status de conformidade do aplicativo	Foi adicionado o tipo de status de Alterações detectadas.	2 de junho de 2022
Apresentando AWS Resilience Hub	AWS Resilience Hub já está disponível. Este guia descreve como usá-lo AWS Resilience Hub para analisar sua infraestrutura, obter recomendações para melhorar a resiliência de seus AWS aplicativos, revisar as pontuações de resiliência e muito mais.	10 de novembro de 2021

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.