aws

用户指南

AWS 弹性中心

AWS 弹性中心: 用户指南

Table of Contents

什么是 AWS Resilience Hub？

AWS Resilience Hub 是您管理和改善应用程序弹性的中心位置 AWS。 AWS Resilience Hub 使您能够定义弹性目标，根据这些目标评估您的弹性态势，并根据Well-Architect AWS ed框架实施改进建议。在内部 AWS Resilience Hub，您还可以创建和运行 Amazon Fault Injection Service 实验，这些实验模仿现实生活中对应用程序的干扰，以帮助您更好地了解依赖关系并发现潜在的弱点。 AWS Resilience Hub 提供持续增强弹性态势所需的所有 AWS 服务和工具的中心位置。 AWS Resilience Hub 与其他服务合作，提供建议并帮助您管理应用程序资源。有关更多信息，请参阅 使用其他服务。

下表提供了所有相关弹性服务的文档链接。

相关的 AWS 弹性服务和参考资料

AWS 弹性服务	文档链接
AWS Elastic Disaster Recovery	弹性灾难恢复
AWS Backup	什么是 AWS Backup
Amazon Route 53 应用程序恢复控制器（Route 53 ARC）	Amazon Route 53 应用程序恢复控制器

主题

AWS Resilience Hub — 弹性管理

AWS Resilience Hub 为您提供了一个定义、验证和跟踪 AWS 应用程序弹性的中心位置。 AWS Resilience Hub 帮助您保护应用程序免受中断，并降低恢复成本以优化业务连续性，从而帮助满足合规性和监管要求。您可以使用 AWS Resilience Hub 执行以下操作：

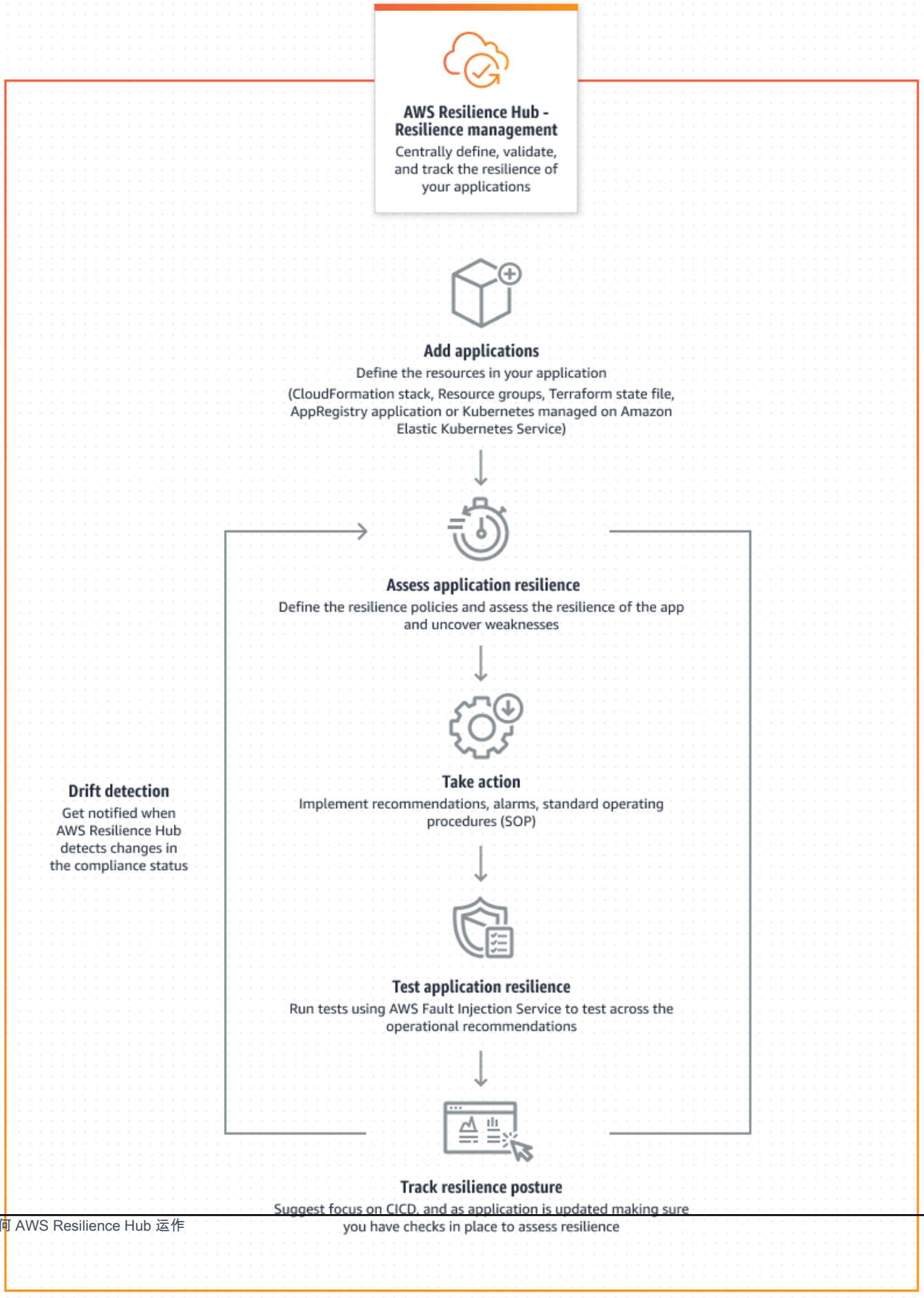
- 分析您的基础架构并获取建议，以提高应用程序的弹性。除了用于提高应用程序弹性的架构指南外，这些建议还提供了满足弹性策略、实施测试、警报和标准操作程序（SOP）的代码，您可以在集成和交付（CI/CD）管道中与应用程序一起部署和运行这些代码。

- 评估不同条件下的恢复时间目标（RTO）和恢复点目标（RPO）目标。
- 优化业务连续性，同时降低恢复成本。
- 在生产中出现问题之前识别并解决问题。

将应用程序部署到生产环境后，您可以添加 AWS Resilience Hub 到 CI/CD 管道中，以便在每个版本发布到生产环境之前对其进行验证。

如何 AWS Resilience Hub 运作

下图简要概述了 AWS Resilience Hub 工作原理。


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

描述

通过从 AWS CloudFormation 堆栈、Terraform 状态文件、Amazon Elastic Kubernetes Service 集群中导入资源来描述您的应用程序，或者您可以从中已经定义的应用程序中进行选择。 AWS Resource Groups AWS Service Catalog AppRegistry

定义

为您的应用程序定义弹性策略。这些策略包括应用程序、基础设施、可用区和区域中断的 RTO 和 RPO 目标。这些目标用于估计应用程序是否符合弹性策略。

评测

描述您的应用程序并向其附加弹性策略后，运行弹性评测。该 AWS Resilience Hub 评估使用 Well-Architect AWS ed Framework 中的最佳实践来分析应用程序的组件并发现潜在的弹性弱点。这些漏洞可能由于基础设施设置不完整、配置错误或需要进一步改进配置的情况造成。要提高弹性，请根据评测报告中的建议更新您的应用程序和弹性策略。建议包括组件、警报、测试和恢复 SOP 的配置。然后，您可以再进行一次评测，并将结果与之前的报告进行比较，以了解弹性在多大程度上得到了改善。重复此过程，直到您的估计工作负载 RTO 和估计的工作负载 RPO 达到您的 RTO 和 RPO 目标。

验证

运行测试以衡量 AWS 资源的弹性以及从应用程序、基础架构、可用区和 AWS 区域 事件中恢复所需的时间。为了衡量弹性，这些测试会模拟您的 AWS 资源中断情况。中断的示例包括网络不可用错误、失效转移、进程停止、Amazon RDS 启动恢复以及可用区问题。

查看和追踪

将 AWS 应用程序部署到生产环境后，您可以使用 AWS Resilience Hub 继续跟踪应用程序的弹性状况。如果发生中断，操作员可以查看中断情况 AWS Resilience Hub 并启动相关的恢复过程。

AWS Resilience Hub — 弹性测试

AWS Resilience Hub 允许您对 AWS 工作负载执行 Amazon 故障注入服务 (AWS FIS) 测试和实验，并保持最佳弹性。这些测试通过创建破坏性事件来给应用程序施加压力，以便您可以观察应用程序的响应情况。 AWS FIS 提供了多个预先构建的场景和大量会造成中断的操作选择。此外，它还包括在生产中运行实验所需的控件和防护机制。控件和防护机制包括用于在满足特定条件时自动回滚或停止实验的选项。要开始使用从AWS Resilience Hub 控制台运行实验，请完成the section called “先决条件”部分中定义的先决条件。 AWS FIS

下表列出了导航窗格中的所有可用 AWS FIS 选项以及相关 AWS FIS 文档的链接，该文档包含从 AWS Resilience Hub 控制台开始使用 AWS FIS 测试的过程。

AWS FIS 导航菜单选项和参考

AWS FIS 导航菜单选项	AWS FIS 文档
弹性测试	创建实验模板
场景库	AWS FIS 图书馆
实验模板	的实验模板 AWS FIS

下表列出了弹性测试部分下拉菜单中的所有可用 AWS FIS 选项，以及相关 AWS FIS 文档的链接，该文档包含从 AWS Resilience Hub 控制台开始使用 AWS FIS 测试的过程。

AWS FIS 下拉菜单选项和参考

AWS FIS 下拉菜单选项	AWS FIS 文档
创建实验模板	创建实验模板
根据场景创建实验	使用场景

AWS Resilience Hub 概念

这些概念可以帮助您更好地了解帮助提高应用程序弹性和防止应用程序中断的方法。 AWS Resilience Hub

故障恢复能力

在指定的时间范围内保持可用性并从软件和操作中断中恢复的能力。

恢复点目标（RPO）滞后

自上一个数据恢复点以来可接受的最长时间。这决定了从上一个恢复点到服务中断之间可接受的数据丢失情况。

恢复时间目标（RTO）

RTO 是指服务中断和服务恢复之间可接受的最大延迟。这决定了当服务不可用时，什么时间段被视为可接受的时间窗口。

估计工作负载恢复时间目标

估计工作负载恢复时间目标（估计工作负载 RTO）是根据导入的应用程序定义估计您的应用程序需要达到的 RTO，然后运行评测。

估计工作负载恢复点目标

估计工作负载恢复点目标（估计工作负载 RPO）是根据导入的应用程序定义估计您的应用程序要达到的 RPO，然后进行评测。

应用程序

AWS Resilience Hub 应用程序是 AWS 受支持资源的集合，这些资源会受到持续监控和评估，以管理其弹性状态。

应用程序组件

一组作为一个单元起作用和失败的相关 AWS 资源。例如，如果您有主数据库和副本数据库，则两个数据库都属于同一个应用程序组件 (AppComponent)。

AWS Resilience Hub 决定哪些 AWS 资源可以属于哪种类型 AppComponent。例如，`DBInstance` 可以属于 `AWS::ResilienceHub::DatabaseAppComponent` 但不属于 `AWS::ResilienceHub::ComputeAppComponent`。

应用程序合规性状态

AWS Resilience Hub 报告应用程序的以下合规性状态类型。

策略已满足

据估计，该应用程序将满足策略中定义的 RTO 和 RPO 目标。其所有组件均符合既定的策略目标。例如，您为跨 AWS 区域的中断选择了 24 小时的 RTO 和 RPO 目标。 AWS Resilience Hub 可以看到您的备份已复制到您的备用区域。您仍然需要保持从备份标准操作程序（SOP）中恢复的状态，并对其进行测试和计时。这包含在操作建议中，也是您的整体弹性分数的一部分。

违反策略

据估计，应用程序无法达到策略中定义的 RTO 和 RPO 目标。其中一个或多个 AppComponents 不符合政策目标。例如，您为跨 AWS 区域的中断选择了 24 小时的 RTO 和 RPO 目标，但您的数据库配置不包括任何跨区域恢复方法，例如全球复制和备份副本。

未评测

该应用程序需要进行评测。目前尚未对其进行评测或跟踪。

检测到的更改

该应用程序有一个新的已发布版本，但尚未经过评测。

弹性偏差

AWS Resilience Hub 运行漂移检测，同时为您的应用程序运行评估以检查其是否符合其弹性策略。为了进行比较， AWS Resilience Hub 使用先前成功评估应用程序时定义的弹性策略。

- 出现偏差 – 表示应用程序违反了其弹性策略并且处于危险之中。
- 未出现偏差 – 表示应用程序的合规性与之前的评测相比没有变化。

弹性评测

AWS Resilience Hub 使用差距和潜在补救措施清单来衡量选定政策在灾难中恢复和延续的有效性。它评估每个应用程序组件或应用程序与策略的合规性状态。该报告包括成本优化建议和对潜在问题的引用。

弹性得分

AWS Resilience Hub 生成一个分数，表明您的应用程序在多大程度上遵循了我们的建议，以满足应用程序的弹性策略、警报、标准操作程序 (SOP) 和测试。

中断类型

AWS Resilience Hub 帮助您评估针对以下类型的停机的弹性：

应用程序

基础设施运行良好，但应用程序或软件堆栈无法按需运行。这可能发生在部署新代码、更改配置、数据损坏或下游依赖项发生故障后。

云基础设施

由于中断，云基础设施无法按预期运行。可能由于一个或多个组件出现本地错误而发生中断。在大多数情况下，这种类型的中断可以通过重新启动、回收或重新加载故障组件来解决。

云基础设施 AZ 中断

一个或多个可用区不可用。可通过切换到不同的可用区来解决此类中断。

云基础设施区域事件

一个或多个区域不可用。这种类型的事件可以通过切换到不同的 AWS 区域来解决。

错误注入实验

AWS Resilience Hub 建议进行测试，以验证应用程序在不同类型的中断情况下的弹性。这些中断包括应用程序、基础设施、可用区（AZ） 或应用程序组件 AWS 区域 事件。

这些实验可让您执行以下操作：

- 注入故障。
- 验证警报是否可以检测到中断。
- 验证恢复程序或标准操作程序（SOP）是否正常运行，以使应用程序从中断中恢复。

SOP 测试可衡量估计工作负载 RTO 和估计工作负载 RPO。您可以测试不同的应用程序配置，并衡量输出 RTO 和 RPO 是否符合策略中定义的目标。

SOP

标准操作程序（SOP）是一组规范性步骤，旨在在发生中断或警报时有效地恢复应用程序。根据应用程序评估， AWS Resilience Hub 建议一组 SOP，建议在中断之前准备、测试和衡量 SOP，以确保及时恢复。

AWS Resilience Hub 支持的资源

AWS Resilience Hub 顶级资源（例如`AWS::RDS::DBInstance`和）完全支持在中断时影响应用程序性能的资源`AWS::RDS::DBCluster`。

要详细了解将所有受支持服务的资源纳入评估所需的权限，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。 AWS Resilience Hub

AWS Resilience Hub 支持来自以下 AWS 服务的资源：

- 计算
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - AWS Lambda
  - Amazon Elastic Kubernetes Service(Amazon EKS)
  - Amazon Elastic Container Service (Amazon ECS)
  - AWS Step Functions
- 数据库
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
- 联网和内容分发
  - Amazon Route 53
  - Elastic Load Balancing
  - 网络地址转换（NAT）
- 存储
  - Amazon Elastic Block Store （Amazon EBS)
  - Amazon Elastic File System (Amazon EFS)
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon FSx for Windows File Server
- 其他
  - Amazon API Gateway
  - Amazon Route 53 应用程序恢复控制器（Route 53 ARC）
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS 弹性灾难恢复

Note

- AWS Resilience Hub 允许您查看每种资源的支持实例，从而提高应用程序资源的透明度。此外，通过识别每种资源的唯一实例，同时在评估过程中发现资源实例，从而 AWS Resilience Hub 提供更准确的弹性建议。有关向应用程序添加资源实例的更多信息，请参阅编辑 AWS Resilience Hub 应用程序资源。
- AWS Resilience Hub 支持 Amazon EKS 和 Amazon AWS Fargate ECS
- AWS Resilience Hub 作为以下服务的一部分，支持 AWS Backup 资源评估：
  - Amazon EBS
  - Amazon EFS
  - Amazon S3
  - Amazon Aurora Global Database
  - Amazon DynamoDB
  - Amazon RDS 数据服务
  - Amazon FSx for Windows File Server
- Amazon Route 53 ARC 仅 AWS Resilience Hub 评估亚马逊 DynamoDB 全球、Elastic Load Balancing、Amazon RDS 和群组。 AWS Auto Scaling
- AWS Resilience Hub 要评估跨区域资源，请将资源分组到单个应用程序组件下。有关每个 AWS Resilience Hub 应用程序组件和分组资源所支持的资源的更多信息，请参阅 将资源分组为 AppComponent。
- 目前，如果 Amazon EKS 集群位于或应用程序是在启用 AWS 了选择加入的区域中创建的，则 AWS Resilience Hub 不支持对 Amazon EKS 集群进行跨区域评估。
- 目前，仅 AWS Resilience Hub 评估以下 Kubernetes 资源类型：
  - 部署
  - ReplicaSets
  - 容器组（pod）

AWS Resilience Hub 忽略以下类型的资源：

- 不影响估计工作负载 RTO 或估计工作负载 RPO 的资源 – 诸如 `AWS::RDS::DBParameterGroup` 资源（此类资源不影响估计工作负载 RTO 或估计工作负载 RPO）将被 AWS Resilience Hub忽略。

- 非顶级资源- AWS Resilience Hub 仅导入顶级资源，因为它们可以通过查询顶级资源的属性来派生其他属性。例如，`AWS::ApiGateway::RestApi` 和 `AWS::ApiGatewayV2::Api` 是 Amazon API Gateway 支持的资源。但是，`AWS::ApiGatewayV2::Stage` 不是顶级资源。因此，它不是由导入的 AWS Resilience Hub。

> **Note**
>
> 不支持的数据来源
>
> - 您无法通过使用 AWS Resource Groups （亚马逊 Route 53 RecordSets 和 API-GW HTTP）和亚马逊 Aurora 全球资源来识别多个资源。如果您想在评测中分析这些资源，则必须手动将资源添加到应用程序中。但是，当您添加 Amazon Aurora 全球资源进行评估时，必须将其与 Amazon RDS 实例的应用程序组件分组。有关资源的更多信息，请参阅 the section called “编辑应用程序资源”。
> - 这些资源可能会影响应用程序的恢复，但 AWS Resilience Hub 目前尚不完全支持它们。AWS Resilience Hub 如果应用程序由 AWS CloudFormation 堆栈、Terraform 状态文件或应用程序支持，则会努力警告用户注意不支持的资源。 AWS Resource Groups AppRegistry

开始使用

本节介绍如何开始安装 AWS Resilience Hub。这包括为账户创建 AWS Identity and Access Management (IAM) 权限。

先决条件

在开始使用 AWS Resilience Hub 之前，您必须满足以下先决条件：

- AWS 账户 — 为要在 AWS Resilience Hub 中使用的每种账户类型（主账户/辅助账户/资源账户）创建一个或多个 AWS 账户。有关创建和管理 AWS 账户的信息，请参阅以下内容：
  - 首次使用 AWS 的用户 — 入门：您是首次使用 AWS 的用户吗？
  - 管理 AWS 账户 — https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management(IAM) 权限 — 创建 AWS 账户后，您必须为已创建的每个账户配置所需的角色和 IAM 权限。例如，如果您创建了一个用于访问应用程序资源的 AWS 账户，则必须为 AWS Resilience Hub 设置一个新角色并配置必要的 IAM 权限，使其能够从您的账户访问应用程序资源。要了解有关 IAM 权限的更多信息，请参阅 the section called “AWS 弹性中心如何与 IAM 配合使用”；有关向角色添加策略的更多信息，请参阅 the section called “使用 JSON 文件定义信任策略”。

  要快速开始向用户、组和角色添加 IAM 权限，您可以使用我们的 AWS 托管策略 (the section called “AWS 托管策略”)。与您自己编写策略相比，使用 AWS 托管策略来覆盖您的 AWS 账户 中可用的常见使用案例则更简单。AWS Resilience Hub 为 AWS 托管策略添加额外权限，以扩展对其他 AWS 服务的支持并包含新功能。因此：
  - 如果您是现有客户，并且希望您的应用程序在评估中使用最新的增强功能，则必须发布该应用程序的新版本，然后运行新的评估。有关更多信息，请参阅以下主题：
    - the section called “发布应用程序的新版本”
    - the section called “运行弹性评估”
  - 如果您未使用 AWS 托管策略向用户、组和角色分配适当的 IAM 权限，则必须手动配置这些权限。有关 AWS 托管策略的更多信息，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

将应用程序添加到 AWS Resilience Hub

AWS Resilience Hub 提供可集成到软件开发生命周期中的弹性评估和验证。 AWS Resilience Hub 通过以下方式帮助您主动准备并保护 AWS 应用程序免受中断：

- 发现弹性弱点。
- 估算目标恢复时间目标（RTO）和恢复点目标（RPO）能否实现。
- 在问题发布到生产环境之前解决问题。

此部分将引导您如何添加应用程序。您可以从现有应用程序、 AWS CloudFormation 堆栈或中收集资源 AWS Resource Groups， AppRegistry 然后创建相应的弹性策略。描述完应用程序后，您可以将其发布到中 AWS Resilience Hub，并生成有关应用程序弹性的评估报告。然后，您可以使用评测中的建议来提高弹性。您可以再运行一次评测，比较结果，然后重复进行，直到估计工作负载 RTO 和估计工作负载 RPO 满足您的 RTO 和 RPO 目标。

主题

步骤 1：从添加应用程序开始

首先， AWS Resilience Hub 请描述您的 AWS 应用程序的详细信息并运行一份报告来评估弹性。

要开始使用，请在 AWS Resilience Hub 主页的 “开始” 下，选择 “添加应用程序”。

要详细了解与之相关的费用和账单 AWS Resilience Hub，请参阅AWS Resilience Hub 定价。

在 AWS Resilience Hub中描述您的应用程序的详细信息

本节介绍如何描述中现有 AWS 应用程序的详细信息 AWS Resilience Hub。

要描述您的应用程序的详细信息

1. 输入应用程序的名称。
2. （可选）输入告警的描述。

下一步

步骤 2：如何管理您的应用程序？

步骤 2：如何管理您的应用程序？

除了 AWS CloudFormation 堆栈 AWS Resource Groups、 AppRegistry 应用程序和 Terraform 状态文件外，您还可以添加位于亚马逊 Elastic Kubernetes Service (Amazon EKS) 集群上的资源。也就是说，AWS 韧性监测中心 允许您将位于 Amazon EKS 集群上的资源添加为可选资源。本部分提供以下选项，可帮助您确定应用程序资源的位置。

- 资源集合 - 如果您要从其中一个资源集合中发现资源，请选择此选项。资源集合包括 AWS CloudFormation 堆栈、 AWS Resource Groups、 AppRegistry 应用程序和 Terraform 状态文件。

  如果选择此选项，则必须完成 the section called “添加资源集合” 中过程之一。
- 仅限 EKS – 如果您想从 Amazon EKS 集群中的命名空间中发现资源，请选择此选项。

  如果选择此选项，则必须完成 the section called “添加 EKS 集群” 中的过程
- 资源集合和 EKS – 如果您想从其中一个资源集合和 Amazon EKS 集群中发现资源，请选择此选项。

  如果选择此选项，请完成 the section called “添加资源集合” 中的过程之一，然后完成 the section called “添加 EKS 集群” 中的过程。

> **Note**
>
> 有关每个应用程序支持的资源数量的信息，请参阅服务限额。

下一步

步骤 3：向 AWS Resilience Hub 应用程序添加资源

步骤 3：向 AWS Resilience Hub 应用程序添加资源

本部分讨论以下选项，您可以使用这些选项来构成应用程序结构的基础：

- the section called “添加资源集合”
- the section called “添加 EKS 集群”

添加资源集合

本部分讨论您用来构成应用程序结构基础的以下方法：

- 使用 AWS CloudFormation 堆栈
- 使用 AWS Resource Groups
- 使用 AppRegistry 应用程序
- 使用 Terraform 状态文件
- 使用现有 AWS Resilience Hub 应用程序

使用 AWS CloudFormation 堆栈

选择包含您要在所描述的应用程序中使用的资源的 AWS CloudFormation 堆栈。堆栈可以来自您 AWS 账户 用来描述应用程序的，也可以来自不同的账户或不同的区域。

要发现构成应用程序结构基础的资源

1. 选择CloudFormation 堆栈以发现基于堆栈的资源。
2. 从 “选择堆栈” 下拉列表中选择与您的 AWS 账户 和地区关联的堆栈。

   要使用位于不同 AWS 账户、不同区域或两者兼而有之的堆栈，请在 “在区域之外 AWS 添加堆栈” 框中输入堆栈的 Amazon 资源名称 (ARN)，然后选择添加堆栈 ARN。有关 ARN 的更多信息，请参阅 AWS 一般参考中的 Amazon Resource Name （ ARN)。

使用 AWS Resource Groups

选择 AWS Resource Groups 包含您要在所描述的应用程序中使用的资源的。

要发现构成应用程序结构基础的资源

1. 选择资源组以发现 AWS Resource Groups 包含这些资源的。
2. 从选择资源组下拉列表中选择资源。

   要使用 AWS Resource Groups 位于不同 AWS 账户、不同区域或两者兼而有之的区域，请在资源组 ARN 框中输入堆栈的 Amazon 资源名称 (ARN)，然后选择添加资源组 ARN。有关 ARN 的更多信息，请参阅 AWS 一般参考中的 Amazon Resource Name （ ARN)。

使用 AppRegistry 应用程序

一次只能添加一个 AppRegistry 应用程序。

选择包含您要在所描述的应用程序中使用的资源的应用程序。 AppRegistry

要发现构成应用程序结构基础的资源

1. 从中创建的应用程序列表中进行选择 AppRegistry。AppRegistry
2. 从 “选择应用程序” 下拉列表中选择在中 AppRegistry创建的应用程序。一次只能选择一个应用程序。

使用 Terraform 状态文件

选择包含您要在所描述的应用程序中使用的 S3 存储桶资源的 Terraform 状态文件。您可以导航到 Terraform 状态文件的位置，也可以提供指向位于不同区域的您有权限访问的 Terraform 状态文件的链接。

> **Note**
>
> AWS Resilience Hub 支持 Terraform 状态文件版本`0.12`及更高版本。

要发现构成应用程序结构基础的资源

1. 选择 Terraform 状态文件以发现您的 S3 存储桶资源。
2. 从选择状态文件部分，选择浏览 S3以导航到 Terraform 状态文件的位置。

   要使用位于不同区域的 Terraform 状态文件，请在 S3 URL 字段中提供指向 Terraform 状态文件位置的链接，然后选择添加 S3 URL。

Terraform 状态文件的限制为 4 兆字节（MB）。

3. 从存储桶部分选择您的 S3 存储桶。
4. 从对象部分中，选择一个密钥，然后选择选择。

使用现有 AWS Resilience Hub 应用程序

要开始进行，请使用现有的应用程序。

要发现构成应用程序结构基础的资源

1. 选择现有应用程序，以从现有应用程序构建应用程序。
2. 从选择现有应用程序下拉列表中选择一个应用程序。

添加 EKS 集群

本部分讨论如何使用 Amazon EKS 集群作为应用程序结构的基础。

> **Note**
>
> 您必须拥有 Amazon EKS 权限和其他 IAM 角色才能连接到 Amazon EKS 集群。有关添加单个账户和跨账户 Amazon EKS 权限以及其他 IAM 角色以连接到集群的更多信息，请参阅以下主题：
>
> - AWS Resilience Hub 访问权限参考
> - the section called “启用对您的 Amazon EKS 集群的 AWS Resilience Hub 访问权限”

选择包含您要在所描述的应用程序中使用的资源的 Amazon EKS 集群和命名空间。Amazon EKS 集群可以来自您用来描述应用程序的，也可以来自不同的账户或不同的区域。 AWS 账户

> **Note**
>
> AWS Resilience Hub 要评估您的 Amazon EKS 集群，您必须在 EKS 集群和命名空间部分中手动向每个 Amazon EKS 集群添加相关的命名空间。命名空间名称必须与 Amazon EKS 集群上的命名空间名称完全匹配。

要添加 Amazon EKS 集群

1. 从选择 EKS 集群下拉列表中选择与您的 AWS 账户 和地区关联的 Amazon EKS 集群。
2. 要使用位于不同 AWS 账户区域或两者兼而有之的 Amazon EKS 集群，请在跨账户或区域框中输入堆栈的亚马逊资源名称 (ARN)，然后选择添加 EKS AR N。有关 ARN 的更多信息，请参阅 AWS 一般参考中的 Amazon Resource Name （ ARN)。

   有关添加访问跨区域 Amazon Elastic Kubernetes Service 集群的权限的更多信息，请参阅 the section called “启用对您的 Amazon EKS 集群的 AWS Resilience Hub 访问权限”。

从所选的 Amazon EKS 集群添加命名空间

1. 从添加命名空间部分中的 EKS 集群和命名空间表中，选择位于 Amazon EKS 集群名称左侧的单选按钮，然后选择更新命名空间。

   您可以通过以下方式识别 Amazon EKS 集群：

   - EKS 集群名称 – 表示所选 Amazon EKS 集群的名称。
   - 命名空间数量 - 表示在 Amazon EKS 集群中选定的命名空间数量。
   - 状态 — 表示您的应用程序中是否包含 AWS Resilience Hub 了来自所选 Amazon EKS 集群的命名空间。您可以使用以下选项识别状态：
     - 必需的命名空间 – 表示您尚未包含 Amazon EKS 集群中的任何命名空间。
     - 命名空间已添加 – 表示您已包含来自 Amazon EKS 集群的一个或多个命名空间。
2. 要添加命名空间，请在更新命名空间对话框中，选择添加新的命名空间。

   更新命名空间对话框将您从 Amazon EKS 集群中选定的所有命名空间显示为可编辑选项。
3. 在更新命名空间对话框中，您有以下编辑选项：

   - 要添加新的命名空间，请选择添加新的命名空间，然后在命名空间框中输入命名空间名称。

     命名空间名称必须与 Amazon EKS 集群上的命名空间名称完全匹配。
   - 要移除命名空间，请选择位于该命名空间旁边的移除。
   - 要将选定的命名空间应用于所有 Amazon EKS 集群，请选择将命名空间应用于所有 EKS 集群。

     如果您选择此选项，则其他 Amazon EKS 集群中先前选择的命名空间将被当前选择的命名空间所覆盖。

4. 要在应用程序中包含更新的命名空间，请选择更新。

下一步

步骤 4：设置 RTO 和 RPO

步骤 4：设置 RTO 和 RPO

您可以使用自己的 RTO/RPO 目标定义新的弹性策略，也可以选择具有预定义的 RTO/RPO 目标的现有弹性策略。如果要使用现有的弹性策略之一，请选择选择现有策略选项，然后从选项项目下拉列表中选择现有的目标应用程序。

定义您自己的 RTO/RPO 目标

1. 选择创建新的弹性策略选项。
2. 输入弹性策略的名称。
3. （可选）输入策略的描述。
4. 在 RTO/RPO 目标部分定义您的 RTO/RPO。

> **Note**
>
> - 我们已经为您的应用程序填充了默认 RTO 和 RPO。您可以立即更改 RTO 和 RPO，也可以在评测应用程序之后更改。
> - AWS Resilience Hub 允许您在弹性策略的 R TO 和 RPO 字段中输入零值。但是，在评测您的应用程序时，可能的最低评测结果接近于零。因此，如果您在 RTO 和 RPO 字段中输入零值，则估计工作负载 RTO 和估计工作负载 RPO 结果将接近零，并且您的应用程序的合规性状态将设置为违反策略。

5. 要为您的基础设施和 AZ 定义 RTO/RPO，请选择向右箭头展开基础设施 RTO 和 RPO 部分。
6. 在 RTO/RPO 目标中，在框中输入一个数值，然后选择该值代表的 RTO 和 RPO 的时间单位。

   在基础设施 RTO 和 RPO 部分中为基础设施和可用区重复这些条目。
7. （可选）如果您有多区域应用程序，并且要定义区域 RTO 和 RPO，请打开区域 - 可选。

   在 RTO 和 RPO 中，在框中输入一个数值，然后选择该值代表的 RTO 和 RPO 的时间单位。

下一步

the section called “步骤 5：设置弹性偏差检测”

步骤 5：偏差检测

AWS 韧性监测中心 允许您设置弹性偏差检测，以便每天评测您的应用程序，并在检测到任何偏差或评测失败时收到通知。

要设置弹性偏差检测

1. 要每天评测您的应用程序，请打开每天自动评测此应用程序。

   如果启用此选项，则每日评测计划仅在以下情况之后开始：

   - 已首次成功手动评测应用程序。
   - 该应用程序配置了适当的 IAM 角色。
   - 如果您的应用程序配置了当前 IAM 用户权限，则您必须创建 `AwsResilienceHubPeriodicAssessmentRole`

     角色，使用 the section called “AWS 弹性中心如何与 IAM 配合使用” 中的相应过程。
2. 要在 AWS Resilience Hub 检测到合规状态存在任何偏差或每日弹性评估失败时收到通知，请打开“获取有关任何弹性政策违规的通知”。

   如果此选项已打开，要接收偏差通知，必须指定一个Amazon Simple Notification Service（Amazon SNS）主题。要提供 Amazon SNS 主题，请在提供 SNS 主题部分，选择选择 SNS 主题选项，然后从选择 SNS 主题下拉列表中选择一个 Amazon SNS 主题。

   > **Note**
   >
   > - 要使 AWS 韧性监测中心 能够向您的 Amazon SNS 主题发布通知，您的 Amazon SNS 主题必须配置相应的权限。有关配置用户权限的信息，请参阅 the section called “允许发布 AWS Resilience Hub 到您的 Amazon SNS 主题”。
   > - 每日评测可能会影响您的运行配额。有关更多信息，请参阅《AWS 一般参考》中的 AWS Resilience Hub 端点和配额。

要使用位于不同 AWS 账户 或不同区域或两者兼而有之的 Amazon SNS 主题，请选择输入 SNS 主题 ARN，然后在 “提供 SNS 主题” 框中输入亚马逊 SNS 主题的亚马逊资源名称 (ARN)。有关 ARN 的更多信息，请参阅 AWS 一般参考中的 Amazon Resource Name （ ARN)。

下一步

步骤 6：设置权限

步骤 6：设置权限

AWS Resilience Hub 允许您为主账户和辅助账户配置必要的权限，以发现和评估资源。但是，您必须单独运行该过程才能为每个账户配置权限。

要配置 IAM 角色和 IAM 权限

1. 要选择用于访问当前账户中资源的现有 IAM 角色，请从选择 IAM 角色下拉列表中选择一个 IAM 角色。

   > **Note**
   >
   > 对于跨账户设置，如果您未在输入 IAM 角色 ARN 框中指定 IAM 角色的 Amazon 资源名称 (ARN) AWS Resilience Hub ，则将使用您从为所有账户选择 IAM 角色下拉列表中选择的 IAM 角色。

   如果您的账户中没有现有 IAM 角色，则可以使用以下选项之一创建 IAM 角色：

   - AWS IAM 控制台 — 如果您选择此选项，则必须完成在 IA M 控制台中创建 AWS Resilience 中心角色中的步骤。
   - AWS CLI — 如果选择此选项，则必须完成 AWS CLI 中的所有步骤。
   - CloudFormation 模板 — 如果您选择此选项，则必须使用相应的 AWS CloudFormation 模板创建角色，具体取决于账户类型（主账户或次要账户）。
2. 选择向右箭头展开从跨账户添加 IAM 角色 - 可选部分。
3. 要从跨账户中选择 IAM 角色，请在输入 IAM 角色 ARN 框中输入 IAM 角色的 ARN。确保您输入的 IAM 角色的 ARN 不属于当前账户。

4. 如果您想使用当前 IAM 用户来发现您的应用程序资源，请选择向右箭头展开使用当前 IAM 用户权限部分，然后选择我知道我必须手动配置权限才能在 AWS Resilience Hub中启用所需功能。

   如果选择此选项，则某些 AWS Resilience Hub 功能（例如弹性漂移检测）可能无法按预期运行，并且您在步骤 1 和步骤 3 中提供的输入将被忽略。

下一步

步骤 8：添加标签

步骤 7：配置应用程序配置参数

本节允许您使用 AWS Elastic Disaster Recovery提供跨区域故障转移支持的详细信息。 AWS Resilience Hub 将使用这些信息来提供弹性建议。

有关 FUOTA 配置参数的更多信息，请参阅 应用程序配置参数。

要添加应用程序配置参数（可选）

1. 要展开应用程序配置参数部分，请选择向右箭头。
2. 在帐户 ID 框中输入失效转移帐户 ID。默认情况下，我们在此字段中预先填充了您使用的账户 ID AWS Resilience Hub，可以更改。
3. 从区域下拉列表中选择失效转移区域。

> **Note**
>
> 如果要禁用此功能，请从下拉列表中选择“–”。

下一步

步骤 8：添加标签

步骤 8：添加标签

为 AWS 资源分配标签或标签，以搜索和筛选您的资源或跟踪您的 AWS 成本。

（可选）要向应用程序添加标签，如果要将一个或多个标签与应用程序关联，请选择添加新标签。有关标签的更多信息，请参阅AWS 一般参考指南中的标记资源。

选择添加应用程序来创建应用程序。

下一步

步骤 9：查看并发布您的 AWS Resilience Hub 应用程序

步骤 9：查看并发布您的 AWS Resilience Hub 应用程序

发布后，您仍可以查看应用程序并编辑其资源。完成后，选择发布以发布应用程序。

有关查看应用程序和编辑其资源的更多信息，请参阅以下内容：

- the section called “查看应用程序摘要”
- the section called “编辑应用程序资源”

下一步

步骤 10：对您的 AWS Resilience Hub 应用程序进行评测

步骤 10：对您的 AWS Resilience Hub 应用程序进行评测

您发布的应用程序将列在摘要页面上。

发布 AWS Resilience Hub 应用程序后，您将被重定向到应用程序摘要页面，您可以在其中进行弹性评估。该评测会根据附加到您的应用程序的弹性策略评估您的应用程序配置。将生成一份评测报告，显示您的应用程序如何根据弹性策略中的目标进行衡量。

要进行弹性评测

1. 在应用程序摘要页面上，选择评测弹性。
2. 在运行弹性评测对话框中，输入报告的唯一名称或使用报告名称框中生成的名称。
3. 选择运行。
4. 收到评测报告已生成的通知后，选择评测选项卡和您的评测以查看报告。
5. 选择查看选项卡以查看您的应用程序的评测报告。

使用 AWS Resilience Hub

AWS Resilience Hub 可帮助您提高 AWS 上的应用程序弹性，并缩短应用程序中断时的恢复时间。

要使用 AWS Resilience Hub，您应：

- 在 AWS Resilience Hub 中描述您的 AWS 应用程序。
- 在 AWS Resilience Hub 中管理您的 AWS 资源。
- 创建有效的弹性策略。
- 管理指示应用程序弹性的评估。
- 管理应用程序的警报、标准操作流程 (SOP) 和测试。

描述和管理 AWS Resilience Hub 应用程序

AWS Resilience Hub 应用程序是 AWS 资源的集合，其结构旨在防止和恢复 AWS 应用程序中断。

要描述 AWS Resilience Hub 应用程序，请提供应用程序名称、来自一个或多个 AWS CloudFormation 堆栈的资源以及适当的弹性策略。您也可以使用任何现有的 AWS Resilience Hub 应用程序作为模板来描述您的应用程序。

描述 AWS Resilience Hub 应用程序后，必须将其发布，以便可对其运行弹性评估。然后，您可以使用评估建议来提高弹性，方法是运行另一项评估，将两项评估的结果进行比较，然后重复该流程，直到估计的工作负载 RTO 和估计的工作负载 RPO 达到 RTO 和 RPO 目标为止。

为了帮助跟踪应用程序的更改，AWS Resilience Hub 显示了应用程序自 AWS Resilience Hub 创建之日起的先前版本。这种可见性可以帮助您查看过去的应用程序配置，并帮助您对当前的应用程序配置做出决定。AWS Resilience Hub 使用以下状态来标识应用程序版本：

- 草稿 — 表示此应用程序版本正在修改中，尚未发布。
- 当前版本 — 表示此应用程序版本是最新发布的版本。AWS Resilience Hub 使用此应用程序版本来运行弹性评估。
- 查看所有版本 — 选择加号 (+) 以只读格式查看所有以前的版本。

您可以通过以下方式从应用程序页面标识您的应用程序：

- 名称 — 您在 AWS Resilience Hub 中指定应用程序名称时所提供的名称。

- 描述 — 您在 AWS Resilience Hub 中指定应用程序描述时所提供的描述。
- 合规性状态 — AWS Resilience Hub 将应用程序状态设置为已评估、未评估、违反策略或检测到更改。
  - 已评估 — AWS Resilience Hub 已对您的应用程序进行评估。
  - 未评估 — AWS Resilience Hub 尚未对您的应用程序进行评估。
  - 违反策略 — AWS Resilience Hub 已确定您的应用程序未达到弹性策略的恢复时间目标 (RTO) 和恢复点目标 (RPO)。在重新评估您的应用程序弹性之前，请查看并使用 AWS Resilience Hub 提供的建议。有关建议的更多信息，请参阅 将应用程序添加到 AWS Resilience Hub。
  - 检测到更改 — AWS Resilience Hub 检测到您的应用程序关联的弹性策略有所更改。您必须重新评估您的应用程序的 AWS Resilience Hub，以确定您的应用程序是否达到弹性策略的目标。
- 按时间表评估 — 资源类型标识了应用程序的组件资源。有关按时间表评估的更多信息，请参阅 应用程序弹性。
  - 处于活动状态 — 表示 AWS Resilience Hub 每天自动评估您的应用程序。
  - 已禁用 — 表示 AWS Resilience Hub 不会每天自动评估您的应用程序，您必须手动评估您的应用程序。
- 弹性偏差状态 — 指示您的应用程序是否与之前的成功评估有所偏差，可设置以下状态之一：
  - 已偏差 — 表示应用程序在之前的成功评估中符合其弹性策略，但现在已经违反了弹性策略，该应用程序目前存在风险。
  - 未偏差 — 表示预计应用程序仍能达到策略中定义的 RTO 和 RPO 目标。
- 估计的工作负载 RTO — 表示应用程序可能的最大估计的工作负载 RTO。此值是自上次成功评估以来所有中断类型的最大估计的工作负载 RTO。
- 估计的工作负载 RPO — 表示应用程序可能的最大估计的工作负载 RPO。此值是自上次成功评估以来所有中断类型的最大估计的工作负载 RTO。
- 上次评估时间 — 指示上次成功评估您的应用程序的日期和时间。
- 创建时间 — 创建应用程序的日期和时间。
- ARN — 应用程序的 Amazon 资源名称（ARN）。有关 ARN 的更多信息，请参阅 AWS 一般参考中的 Amazon Resource Name (ARN)。

> **Note**
>
> 只有在您将 Amazon ECR 用于映像存储库时，AWS Resilience Hub 才能全面评估跨区域 Amazon ECS 资源的弹性。

此外，您还可以使用应用程序页面中的以下选项之一来筛选应用程序列表：

- 查找应用程序 — 输入您的应用程序名称，以按应用程序名称筛选结果。
- 按日期和时间范围筛选上次评估时间 — 要应用此筛选条件，请选择日历图标并选择以下选项之一，以按与时间范围匹配的结果进行筛选：
  - 相对范围 — 选择可用选项之一，然后选择应用。

    如果选择自定义范围选项，请在输入持续时间框中输入持续时间，然后从时间单位下拉列表中选择相应的时间单位，然后选择应用。
  - 绝对范围 — 要指定日期和时间范围，请提供开始时间和结束时间，然后选择应用。

以下主题演示了描述 AWS Resilience Hub 应用程序的不同方法以及管理方式。

主题

查看 AWS Resilience Hub 应用程序摘要

AWS Resilience Hub 控制台中的应用程序摘要页面概述了您的应用程序信息和弹性运行状况。

查看应用程序摘要

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择应用程序名称。

应用程序摘要页面包含以下部分。

主题

- 详细信息
- 应用程序弹性
- 已实施的警报
- 已实施的实验

详细信息

应用程序摘要的详细信息部分显示应用程序的选项摘要。

- 应用程序状态 — 指示您的应用程序是否处于运行状态。
- 描述 — 关于应用程序的描述。
- 合规性状态 — 指示您的应用程序的合规性状态。
- 上次评估时间 — 指示上次评估您的应用程序的日期和时间。
- 弹性策略 — 显示附加到您的应用程序的弹性策略的名称。有关弹性策略的更多信息，请参阅 管理弹性策略。
- 按时间表评估 — 指示每日评估处于活动状态还是非活动状态。
- 弹性偏差状态 — 指示您的应用程序是否与之前的成功评估有所偏差。
- 上次偏差时间 — 指示检查您的应用程序是否存在偏差的日期和时间。

更新按时间表评估

1. 要更新按时间表评估应用程序，请从操作中选择更新弹性偏差检测。
2. 要更新弹性偏差检测，请完成 步骤 5：偏差检测 中的步骤，然后返回到此过程。
3. 选择更新。

> **Note**
>
> 要在现有应用程序上激活弹性偏差检测，您必须在首次启用弹性偏差检测功能后手动运行评估。有关运行评估的更多信息，请参阅 运行弹性评估。

应用程序弹性

应用程序弹性部分显示的指标来自最新的应用程序弹性评估。

弹性得分

弹性得分可帮助您对是否准备好应对潜在中断进行量化。该评分反映了您的应用程序在满足应用程序弹性策略、警报、标准操作流程 (SOP) 和测试要求方面遵从 AWS Resilience Hub 建议的程度。

您的应用程序可以达到的最大弹性得分为 100%。评分代表了预定义的时间段内运行的所有建议测试。它表示测试正在启动正确的警报，并且警报启动了正确的 SOP。

例如，假设 AWS Resilience Hub 建议在一次测试中启动一次警报和一个 SOP。当测试运行时，警报会启动关联的 SOP，则表示运行成功。有关弹性得分的更多信息，请参阅 了解弹性分数。

随时间推移的弹性得分

采用随时间推移的弹性得分，您可以查看过去 30 天内的应用程序弹性图表。虽然下拉菜单可以列出 10 个应用程序，但 AWS Resilience Hub 一次只能显示最多四个应用程序的图表。有关按时间表评估的更多信息，请参阅 步骤 5：偏差检测 。

> **Note**
>
> AWS Resilience Hub 不会同时运行多个按时间表评估。因此，您可能需要稍后返回到随时间推移的弹性得分图表，以查看应用程序的每日评估情况。

AWS Resilience Hub 还使用 Amazon CloudWatch 生成这些图表。选择在 CloudWatch 中查看指标，以在 CloudWatch 控制面板中创建和查看有关应用程序弹性的更精细的信息。有关 CloudWatch 的更多信息，请参阅 Amazon CloudWatch 用户指南中的使用控制面板。

已实施的警报

应用程序摘要中的已实施的警报部分列出了您在 Amazon CloudWatch 中为监控应用程序而设置的警报。有关警报的更多信息，请参阅 管理警报。

已实施的实验

应用程序摘要中的错误注入实验部分显示了错误注入实验的列表。有关错误注入实验的更多信息，请参阅 Amazon 错误注入服务实验。

编辑 AWS Resilience Hub 应用程序资源

请确保更新您的应用程序描述且其与您的实际 AWS 应用程序和资源相匹配，以获得准确有用的弹性评测。评测报告、验证和建议均基于列出的资源。如果您需要在 AWS 应用程序中添加或删除资源，应在 AWS Resilience Hub 中反映这些更改。

AWS Resilience Hub 提供有关应用程序源的透明度。您可以识别和编辑应用程序中的资源和应用程序源。

> **Note**
>
> 编辑资源只会修改应用程序的 AWS Resilience Hub 引用。不会对您的实际资源进行任何更改。

您可以添加缺失的资源、修改现有资源或移除不需要的资源。资源分为逻辑应用程序组件 (AppComponent)。您可以编辑 AppComponent 以更好地反映应用程序的结构。

通过编辑应用程序的草稿版本并将更改发布到新（发布）版本来添加或更新应用程序资源。AWS Resilience Hub 使用应用程序的发布版本（包括更新的资源）来运行弹性评测。

评测应用程序的弹性

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择您要编辑的应用程序的名称。
3. 从操作菜单中选择评测弹性。
4. 在运行弹性评测对话框中，输入报告的唯一名称或使用报告名称框中生成的名称。
5. 选择 运行。
6. 收到评测报告已生成的通知后，选择评测选项卡和您的评测以查看报告。
7. 选择应用程序评测报告的审核选项卡。

更新应用程序的弹性偏差检测

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择您要针对其启用或禁用弹性偏差检测的应用程序。
3. 从操作中，选择更新弹性偏差检测。
4. 要更新弹性偏差检测，请完成 步骤 5：偏差检测 中的步骤，然后返回到此过程。
5. 选择更新。

更新应用程序的安全权限

1. 在导航窗格中，选择 Applications（应用程序）。

2. 在应用程序页面上，选择要更新其安全权限的应用程序。
3. 从操作中，选择更新权限。
4. 要更新安全权限，请完成 步骤 6：设置权限 中的步骤，然后返回到此过程。
5. 选择保存并更新。

要将弹性策略附加到您的应用程序

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择您要编辑的应用程序的名称。
3. 从操作菜单中，选择附加弹性策略。
4. 在附加策略对话框中，从选择弹性策略下拉列表中选择弹性策略。
5. 选择 Attach (附加)。

要编辑应用程序的输入源、资源和应用程序组件

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择您要编辑的应用程序的名称。
3. 选择应用程序结构选项卡。
4. 在版本前选择加号 +，然后选择处于草稿状态的应用程序版本。

5. 要编辑应用程序的输入源、资源和 AppComponent，请完成以下过程中的步骤。

要编辑应用程序的输入源

1. 要编辑应用程序的输入源，请选择输入源选项卡。

   输入源部分列出了您的应用程序资源的所有输入源。您可以通过以下方式识别输入源：

   - 源名称 – 输入源的名称。选择源名称以在相应的应用程序中查看其详细信息。对于手动添加的输入源，该链接将不可用。例如，如果您选择了从 AWS CloudFormation 堆栈导入的源名称，系统会将您重定向到 AWS CloudFormation 上的堆栈详细信息页面。
   - 源 ARN – 输入源的 Amazon 资源名称 (ARN)。选择 ARN 以在相应的应用程序中查看其详细信息。对于手动添加的输入源，该链接将不可用。例如，如果您选择从 AWS CloudFormation 堆栈导入的 ARN，您将被重定向到 AWS CloudFormation 控制台上的堆栈详情页面。

- 源类型 - 输入源的类型。输入源包括 Amazon EKS 集群、AWS CloudFormation 堆栈、AppRegistry 应用程序、AWS Resource Groups、Terraform 状态文件和手动添加的资源。
- 关联资源 - 与输入源关联的资源数量。在资源选项卡中选择一个数字，即可查看输入源的所有关联资源。

2. 要向应用程序添加输入源，请从输入源部分中选择添加输入源。有关添加社交 IdP 的更多信息，请参阅the section called “步骤 3：向 AWS Resilience Hub 应用程序添加资源”。
3. 要编辑输入源，请选择“输入源”，然后从操作中选择以下选项之一：

- 重新导入输入源（最多 5 个）- 最多重新导入五个选定的输入源。
- 删除输入源 - 删除选定的输入源。

  要发布应用程序，则应用程序必须至少包含一个输入源。如果删除所有输入源，则将禁用发布新版本。

编辑应用程序的资源

1. 要编辑应用程序的资源，请选择资源选项卡。

> **Note**
>
> 要查看未评测的资源列表，请选择查看未评测的资源。

资源部分列出了您选择用作应用程序描述模板的应用程序资源。为了增强您的搜索体验，AWS Resilience Hub 根据多个搜索条件对资源进行了分组。这些搜索条件包括 AppComponent 类型、不支持的资源和排除的资源。要根据资源表中的搜索条件筛选资源，请选择每个搜索条件下方的数字。

您可以按 前缀识别这些资源：

- 逻辑 ID — 逻辑 ID 是用于标识 AWS CloudFormation 堆栈、Terraform 状态文件、手动添加的应用程序、AppRegistry 应用程序或 AWS Resource Groups 中的资源的名称。

> **Note**
>
> - Terraform 允许您对不同的资源类型使用相同的名称。因此，对于共享相同名称的资源，您会在逻辑 ID 的末尾看到“- 资源类型”。

- 要查看所有应用程序资源的实例，请选择逻辑 ID 前的加号 (+)。要查看应用程序资源的所有实例，请选择每个资源的“逻辑 ID”前的加号 (+)。

  有关支持的资源类型的更多信息，请参阅 the section called “支持的 AWS Resilience Hub 资源”。

- 资源类型 - 资源类型标识应用程序的组件资源。例如，`AWS::EC2::Instance` 声明 Amazon EC2 实例。有关对 AppComponent 资源进行分组的更多信息，请参阅 将资源分组为 AppComponent。
- 源名称 – 输入源的名称。选择源名称以在相应的应用程序中查看其详细信息。对于手动添加的输入源，该链接将不可用。例如，如果您选择了从 AWS CloudFormation 堆栈导入的源名称，系统会将您重定向到 AWS CloudFormation 上的堆栈详细信息页面。
- 源类型 - 输入源的类型。输入源包括 AWS CloudFormation 堆栈、AppRegistry 应用程序、AWS Resource Groups、Terraform 状态文件和手动添加的资源。

  > **Note**
  >
  > 要编辑您的 Amazon EKS 集群，请完成要编辑 AWS Resilience Hub 应用程序的输入源过程中的步骤。

- 源堆栈 - 包含资源的 AWS CloudFormation 堆栈。此列取决于您选择的应用程序结构的类型。
- 物理 ID — 分配给资源的实际标识符，如 Amazon EC2 实例 ID 或 S3 存储桶名称。
- 已包含 — 指示 AWS Resilience Hub 是否将这些资源包含在应用程序中。
- 可评测 – 这表示 AWS Resilience Hub 是否会评测您的资源的弹性。
- AppComponents – 在发现该资源的应用程序结构时分配给该资源的 AWS Resilience Hub 组件。
- 名称 — 应用程序资源的名称。
- 账户 — 拥有物理资源的 AWS 账户。

2. 要查找未列出的资源，请在搜索框中输入资源逻辑 ID。
3. 要从应用程序中删除资源，请选择该资源，然后从操作中选择排除资源。
4. 要解析应用程序上的资源，请选择刷新资源。
5. 要修改现有的应用程序资源，请完成以下步骤：

   a. 选择资源，然后从操作中选择更新堆栈。

b. 在更新堆栈页面中，要更新您的资源，请完成 步骤 3：向 AWS Resilience Hub 应用程序添加资源 中的相应步骤，然后返回到此过程。

c. 选择 Save（保存）。

6. 要向应用程序添加资源，请从操作中选择添加资源，然后完成以下步骤：

a. 从资源类型下拉列表中，选择至少一种资源类型。

b. 从 AppComponen 下拉列表中选择一个 AppComponent。

c. 在资源名称框中输入资源逻辑 ID。

d. 在资源标识符框中输入物理资源 ID、资源名称或资源 ARN。

e. 选择 Add（添加）。

7. 要编辑资源名称，请选择一个资源，从操作中选择编辑资源名称，然后完成以下步骤：

a. 在资源名称框中输入资源逻辑 ID。

b. 选择 Save（保存）。

8. 要编辑资源标识符，请选择一个资源，从操作中选择编辑资源标识符，然后完成以下步骤：

a. 在资源标识符框中输入物理资源 ID、资源名称或资源 ARN。

b. 选择 Save（保存）。

9. 要更改 AppComponent，请选择一个资源，从操作中选择更改 AppComponent，然后完成以下步骤：

a. 从 AppComponen 下拉列表中选择一个 AppComponent。

b. 选择 Add（添加）。

10. 要删除资源，请选择一个资源，然后从操作中选择删除资源。

11. 要包含资源，请选择资源，然后从操作中选择包含资源。

要编辑应用程序的 AppComponent

1. 要编辑应用程序的应用程序组件，请选择 AppComponent 选项卡。

> **Note**
>
> 有关对 AppComponent 资源进行分组的更多信息，请参阅 将资源分组为 AppComponent。

AppComponent 部分列出了资源分组归入的所有逻辑组件。您可以通过以下方式识别 AppComponent：

- AppComponent 名称 - 在发现该资源的应用程序结构时分配给该资源的 AWS Resilience Hub 组件的名称。
- AppComponent 类型 - AWS Resilience Hub 组件的类型。
- 源名称 – 输入源的名称。选择源名称以在相应的应用程序中查看其详细信息。例如，如果您选择了从 AWS CloudFormation 堆栈导入的源名称，系统会将您重定向到 AWS CloudFormation 上的堆栈详细信息页面。
- 资源计数 - 与输入源关联的资源数量。在资源选项卡中选择一个数字，即可查看输入源的所有关联资源。

2. 要创建 AppComponent，请从操作菜单中选择创建新 AppComponent，然后完成以下步骤：
   a. 在 AppComponent 名称框中输入 AppComponent 的名称。作为参考，我们在此字段中预先填充了示例名称。
   b. 从 AppComponent 类型下拉列表中选择 AppComponent 的类型。
   c. 选择 Save（保存）。
3. 要编辑 AppComponent，请选择一个 AppComponent，然后从操作中选择编辑 AppComponent。
4. 要删除 AppComponent，请选择一个 AppComponent，然后从操作中选择删除 AppComponent。

对资源列表进行更改后，您将收到一条警报，表明已对您的应用程序的草稿版本进行了更改。要运行准确的弹性评测，您必须发布新版本的应用程序。有关如何发布新版本的更多信息，请参阅 发布 AWS Resilience Hub 应用程序的新版本。

将资源分组为 AppComponent

A AppComponent n 是一组相关 AWS 资源，它们作为一个单元起作用和失败。例如，如果您有主数据库和副本数据库，则两个数据库都属于同一个应用程序组件 (AppComponent)。AWS Resilience Hub 有管理哪些 AWS 资源可以属于哪种类型的规则 AppComponent。例如，`DBInstance` 可以属于 `AWS::ResilienceHub::DatabaseAppComponent` 但不属于 `AWS::ResilienceHub::ComputeAppComponent`。

将应用程序 AWS Resilience Hub 与 AWS CloudFormation 堆栈、Terraform 状态文件 AWS Resource Groups、Amazon Elastic Kubernetes Service 集群或 AWS Resilience Hub 应用程序一起导 AppComponent入时 AppRegistry ，会尽最大努力将相关资源分组到相同的资源中，但可能并

不总是百分之百准确。您最了解应用程序的架构，因此您可以将已经按其分组的资源重新组合 AWS Resilience Hub 为不同的 AppComponent资源。例如，如果您的 AWS CloudFormation 堆栈中有三个 EC2 实例，则为 AppComponent 每个 EC2 实例 AWS Resilience Hub 创建一个实例，但所有三个 EC2 实例都可能运行相同的应用程序软件。在这种情况下，正确的选择是将三个 EC2 实例重新分组到单个 ComputeAppComponent 下。在重新分组资源时，您只应将资源重新组合为单个资源。AppComponent您也可以展开资源列表，将未分组的资源组合为。 AppComponent

它们 AWS Resilience Hub AppComponents 支持以下资源：

- 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**
>
> 目前，仅 AWS Resilience Hub 支持适用于 Windows File Server 的亚马逊 FSx。

  - `AWS::S3::Bucket`

以下是正确分组的示例：

- 将主数据库和副本分组到一个 AppComponent数据库下。
- 将 Amazon S3 存储桶及其复制分组到一个存储桶下 AppComponent。
- 将运行相同应用程序的 Amazon EC2 实例分组到一个实例下 AppComponent。
- 将 Amazon SQS 队列及其死信队列分组到一个队列下。 AppComponent
- 将一个区域的 Amazon ECS 服务分组到一个区域，将另一个区域的 Amazon ECS 服务故障转移到一个区域下 AppComponent。

> **Note**
>
> AWS Resilience Hub 需要进行正确的分组，以便它可以计算估计的工作负载 RTO 和估计的工作负载 RPO 以生成建议。

将资源分配给 AppComponent

1. 在导航窗格中，选择 应用程序。
2. 在应用程序页面上，选择含有要重新分组的资源的应用程序名称。
3. 选择应用程序结构选项卡。
4. 在版本下，选择处于草稿状态的应用程序版本。

5. 选择资源选项卡。
6. 选择要重新分组的资源。
7. 从 “操作” 中选择 “更改” AppComponent。

   将显示 AppComponent “更改” 对话框。
8. 要 AppComponent 从分AppComponent区中删除当前，请在显示您当前 AppComponent 姓名的标签的右上角选择 X。
9. 要将资源分组为不同的资源 AppComponent，请 AppComponent从 “选择” AppComponent 下拉列表中选择不同的资源。
10. 选择 添加。
11. AppComponents 从AppComponents选项卡中删除所有空白。
12. 选择 새 버전 발행。
13. 选择应用程序结构选项卡。
14. 要查看应用程序的已发布版本，请完成以下步骤：

    a. 在版本选项卡下，选择处于当前版本状态的应用程序版本。

    b. 选择资源选项卡。

对资源进行分组

1. 在导航窗格中，选择 应用程序。
2. 在应用程序页面上，选择包含要分组的资源的应用程序名称。
3. 选择应用程序结构选项卡。
4. 在版本选项卡下，选择处于草稿状态的应用程序版本。
5. 选择资源选项卡。
6. 选择要分组的资源。

   > **Note**
   >
   > 您不能选择手动添加的资源。

7. 选择操作，然后选择对资源进行分组。

   将显示 AppComponent “合并” 窗口。

8. AppComponent 从 “选择” AppComponent 下拉列表中选择要对资源进行分组的。
9. 选择 保存。
10. 选择 새 버전 발행。
11. 选择应用程序结构选项卡。
12. 要查看应用程序的已发布版本，请完成以下步骤：

    a. 在版本选项卡下，选择处于当前版本状态的应用程序版本。

    b. 选择资源选项卡。

发布 AWS Resilience Hub 应用程序的新版本

按照 编辑 AWS Resilience Hub 应用程序资源 中所述对 AWS Resilience Hub 应用程序资源进行更改后，必须发布应用程序的新版本才能进行准确的弹性评估。此外，如果您在应用程序中添加了新的建议警报、SOP 和测试，则可能需要发布应用程序的新版本。

发布应用程序的新版本

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择应用程序名称。
3. 选择应用程序结构选项卡。
4. 选择 Publish new version。
5. 在发布版本对话框的名称框中，输入应用程序版本的名称，也可以使用 AWS Resilience Hub 建议的默认名称。
6. 选择 Publish。

   在发布应用程序的新版本时，该版本将成为您运行弹性评估时所评估的版本。此外，在您进行任何更改之前，草稿版本将与已发布版本相同。

在您发布应用程序的新版本后，我们建议您运行新的弹性评估报告，以确认您的应用程序仍然符合您的弹性策略。有关运行评估的信息，请参阅 运行和管理 AWS Resilience Hub 弹性评估。

查看所有 AWS Resilience Hub 应用程序版本

为了帮助跟踪应用程序的更改，AWS Resilience Hub 显示了应用程序自 AWS Resilience Hub 创建之日起的先前版本。

查看应用程序的所有版本

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择应用程序名称。
3. 选择应用程序结构选项卡。
4. 要查看应用程序的所有先前版本，请选择查看所有版本前的加号 (+)。AWS Resilience Hub 分别使用草稿和当前版本状态来表示应用程序的草稿版本和最近发布的版本。您可以选择应用程序的任何版本来查看其资源、AppComponent、输入源和其他相关信息。

   此外，您还可以使用以下选项之一来筛选列表：

   - 按版本名称筛选 — 输入名称以按应用程序版本名称筛选结果。
   - 按日期和时间范围筛选 — 要应用此筛选条件，请选择日历图标并选择以下选项之一，以按与时间范围匹配的结果进行筛选：
     - 相对范围 — 选择可用选项之一，然后选择应用。

       如果选择自定义范围选项，请在输入持续时间框中输入持续时间，然后从时间单位下拉列表中选择相应的时间单位，然后选择应用。
     - 相对范围 — 要指定日期和时间范围，请提供开始时间和结束时间，然后选择应用。

查看 AWS Resilience Hub 应用程序资源

查看应用程序资源

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择要更新其安全权限的应用程序。
3. 从操作中选择查看资源。

   在资源选项卡中，您可以通过以下方式在资源表中标识资源：

   - 逻辑 ID — 逻辑 ID 是用于标识 AWS CloudFormation 堆栈、Terraform 状态文件、手动添加的应用程序、AppRegistry 应用程序或 AWS Resource Groups 中的资源的名称。

     > **Note**
     >
     > - Terraform 允许您对不同的资源类型使用相同的名称。因此，对于共享相同名称的资源，您会在逻辑 ID 的末尾看到“- 资源类型”。

- 要查看所有应用程序资源的实例，请选择逻辑 ID 前的加号 (+)。要查看应用程序资源的所有实例，请选择每个资源的“逻辑 ID”前的加号 (+)。

  有关支持的资源类型的更多信息，请参阅 the section called “支持的 AWS Resilience Hub 资源”。

- 状态 — 指示 AWS Resilience Hub 是否会评估您的资源弹性。
- 资源类型 - 资源类型标识应用程序的组件资源。例如，`AWS::EC2::Instance` 声明 Amazon EC2 实例。有关对 AppComponent 资源进行分组的更多信息，请参阅 将资源分组为 AppComponent。
- 源名称 — 输入源的名称。选择源名称以在相应的应用程序中查看其详细信息。对于手动添加的输入源，该链接将不可用。例如，如果您选择了从 AWS CloudFormation 堆栈导入的源名称，系统会将您重定向到 AWS CloudFormation 上的堆栈详细信息页面。
- 源类型 — 输入源的类型。
- AppComponent 类型 — 输入源的类型。输入源包括 AWS CloudFormation 堆栈、AppRegistry 应用程序、AWS Resource Groups、Terraform 状态文件和手动添加的资源。

  > **Note**
  >
  > 要编辑您的 Amazon EKS 集群，请完成要编辑 AWS Resilience Hub 应用程序的输入源过程中的步骤。

- 物理 ID — 分配给资源的实际标识符，如 Amazon EC2 实例 ID 或 S3 存储桶名称。
- 已包含 — 指示 AWS Resilience Hub 是否将这些资源包含在应用程序中。
- AppComponents — 在发现某个资源的应用程序结构时分配给该资源的 AWS Resilience Hub 组件。
- 名称 — 应用程序资源的名称。
- 账户 — 拥有物理资源的 AWS 账户。

4. 选择保存并更新。

删除 AWS Resilience Hub 应用程序

在达到十个应用程序的最大限制后，必须先删除一个或多个应用程序，然后才能添加更多应用程序。

删除应用程序

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择要删除的应用程序。
3. 选择 Actions (操作)，然后选择 Delete application (删除应用程序)。
4. 要确认删除，请在删除框中输入删除，然后选择删除。

应用程序配置参数

AWS Resilience Hub 提供了一种输入机制，用于收集与您的应用程序关联的资源相关的其他信息。利用这些信息，AWS Resilience Hub 将更深入地了解您的资源并提供更好的弹性建议。

应用程序配置参数章节列出了对 AWS Elastic Disaster Recovery 提供跨区域失效转移支持的所有配置参数。您可以通过以下方式标识配置参数：

- 主题 — 指出已配置的应用程序区域。例如，失效转移配置。
- 目的 — 指明 AWS Resilience Hub 要求提供信息的原因。
- 参数 — 表示应用程序特定区域的详细信息，这些详细信息 AWS Resilience Hub 将用于为您的应用程序提供建议。当前，此参数仅使用一个失效转移区域和一个关联账户的键值。

更新应用程序配置参数

本部分允许您更新您的 AWS Elastic Disaster Recovery 的配置参数并发布应用程序，以包含更新后的弹性评估参数。

更新应用程序配置参数

1. 在导航窗格中，选择 Applications（应用程序）。
2. 在应用程序页面上，选择您要编辑的应用程序的名称。
3. 选择应用程序配置参数选项卡。
4. 选择更新。
5. 在帐户 ID 框中输入失效转移帐户 ID。
6. 从区域下拉列表中选择失效转移区域。

> **Note**
>
> 如果要禁用此功能，请从下拉列表中选择“-”。

7. 选择更新并发布。

管理弹性策略

本部分介绍如何为您的应用程序创建弹性策略。正确设置弹性策略使您能够了解应用程序的弹性状态。弹性策略包含信息和目标，您可以使用这些信息和目标来评测您的应用程序是否预计可以从中断类型（例如软件、硬件、可用区或 AWS 区域）中恢复。这些策略不会更改或影响实际应用程序。多个应用程序可以具有相同的弹性策略。

创建弹性策略时，您可定义目标：恢复时间目标 (RTO) 和恢复点目标 (RPO)。这些目标决定了应用程序是否符合弹性策略。将策略附加到您的应用程序并运行弹性评测。您可以为您的组合中不同类型的应用程序创建不同的策略。例如，实时交易应用程序的弹性策略将与月度报告应用程序不同。

> **Note**
>
> AWS Resilience Hub 允许您在弹性策略的 RTO 和 RPO 字段中输入零值。但是，在评测您的应用程序时，可能的最低评测结果接近于零。因此，如果您在 RTO 和 RPO 字段中输入零值，则估计工作负载 RTO 和估计工作负载 RPO 结果将接近零，并且您的应用程序的合规性状态将设置为违反策略。

该评测会根据附加的弹性策略评估您的应用程序配置。在该进程结束时，AWS Resilience Hub 会提供您的应用程序如何根据弹性策略中的恢复目标进行衡量的评测。

您可以在“应用程序”中创建弹性策略，也可以在“弹性策略”中创建。您可以访问有关您的策略的相关详细信息，也可以对其进行修改和删除。

AWS Resilience Hub 使用您的 RTO 和 RPO 目标来衡量针对以下潜在中断类型的弹性：

- 应用程序 – 丢失所需的软件服务或进程。
- 云基础设施 – 丢失硬件，例如 EC2 实例。
- 云基础设施可用区 (AZ) – 一个或多个可用区不可用。
- 云基础设施区域 - 一个或多个区域不可用。

AWS Resilience Hub 使您能够创建自定义的弹性策略或使用我们建议的开放标准弹性策略。创建自定义策略时，请命名和描述您的策略，并选择定义您的策略的相应级别或层级。这些层级包括：基础 IT 核心服务、关键任务、关键、重要和非关键。

选择适合您的应用程序类别的层级。例如，您可以将实时交易系统归类为关键系统，而将月度报告应用程序归类为非关键应用程序。使用我们的标准策略时，您可以选择具有预配置层级的弹性策略以及按中断类型划分的 RTO 和 RPO 目标值。如有必要，您可以更改层级以及 RTO 和 RPO 目标。

您可以在“弹性策略”中创建弹性策略，也可以在描述新应用程序时创建弹性策略。

创建弹性策略

在 AWS Resilience Hub 中，您可以创建弹性策略。弹性策略包含信息和目标，您可以使用这些信息和目标来评测您的应用程序是否可以从中断类型（例如软件、硬件、可用区或 AWS 区域）中恢复。这些策略不会更改或影响实际应用程序。多个应用程序可以具有相同的弹性策略。

创建弹性策略时，您可定义恢复时间目标 (RTO) 和恢复点目标 (RPO) 目标。在运行评测时，AWS Resilience Hub 确定应用程序是否预计符合弹性策略中定义的目标。

该评测会根据附加的弹性策略评估您的应用程序配置。在进程结束时，AWS Resilience Hub 会提供您的应用程序如何根据弹性策略中的目标进行衡量的评测。

> **Note**
>
> AWS Resilience Hub 允许您在弹性策略的 RTO 和 RPO 字段中输入零值。但是，在评测您的应用程序时，可能的最低评测结果接近于零。因此，如果您在 RTO 和 RPO 字段中输入零值，则估计工作负载 RTO 和估计工作负载 RPO 结果将接近零，并且您的应用程序的合规性状态将设置为违反策略。

您可以在“应用程序”中创建弹性策略，也可以在“弹性策略”中创建。您可以访问有关您的策略的相关详细信息，也可以对其进行修改和删除。

在“应用程序”中创建弹性策略

1. 在左侧的导航菜单中，选择应用程序。
2. 通过 the section called “步骤 8：向应用程序添加标签”，从 the section called “步骤 1：从添加应用程序开始” 完成这些过程。
3. 在弹性策略部分，选择创建弹性策略。

创建弹性策略页面将显示。

4. 在选择创建方法部分，选择创建策略。
5. 输入策略的名称。
6. （可选）输入策略的描述。
7. Master key (主密钥) 从下拉列表中选择以下选项之一：
   - 基础 IT 核心服务
   - 关键任务
   - 重大
   - 重要提示
   - 非关键
8. 对于 RTO 和 RPO 目标，在客户应用程序 RTO 和 RPO 下，在框中输入一个数值，然后选择该值所代表的时间单位。

   在基础设施和可用区的基础设施 RTO 和 RPO 下重复这些条目。
9. （可选）如果您有多区域应用程序，则可能需要定义区域的 RTO 和 RPO 目标。

   启用区域。对于区域 RTO 和 RPO 目标，在客户应用程序 RTO和 RPO 下，在框中输入一个数值，然后选择该值表示的时间单位。
10. （可选）如果要添加标签，则可以在稍后继续创建策略时执行此操作。有关标签的更多信息，请参阅AWS一般参考指南中的标记资源。
11. 选择 Create（创建）以创建策略。

在“弹性策略”中创建弹性策略

1. 从左侧导航菜单中，选择 Policies (策略)。
2. 在弹性策略部分，选择创建弹性策略。

   创建弹性策略页面将显示。
3. 输入策略的名称。
4. （可选）输入策略的描述。
5. 请选择以下选项之一。
   - 基础 IT 核心服务

- 关键任务
- 重大
- 重要提示
- 非关键

6. 对于 RTO 和 RPO 目标，在客户应用程序 RTO 和 RPO下，在框中输入一个数值，然后选择该值所代表的时间单位。

   在基础设施和可用区的基础设施 RTO 和 RPO 下重复这些条目。

7. （可选）如果您有多区域应用程序，则可能需要定义区域的 RTO 和 RPO 目标。

   启用区域。对于 RTO 和 RPO 目标，在客户应用程序 RTO 和 RPO下，在框中输入一个数值，然后选择该值所代表的时间单位。

8. （可选）如果要添加标签，则可以在稍后继续创建策略时执行此操作。有关标签的更多信息，请参阅AWS一般参考指南中的标记资源。

9. 选择 Create（创建）以创建策略。

根据建议的策略创建弹性策略

1. 从左侧导航菜单中，选择 Policies (策略)。
2. 在选择创建方法部分，选择根据建议的策略选择策略。
3. 在弹性策略部分，选择创建弹性策略。

   创建弹性策略页面将显示。

4. 输入弹性策略的名称。
5. （可选）输入策略的描述。
6. 在建议的弹性策略部分下，查看并选择以下预先确定的弹性策略层级之一：

   - 非关键应用程序
   - 重要应用程序
   - 关键应用程序
   - 全局关键应用程序
   - 关键任务应用程序
   - 全局关键任务应用程序
   - 基础核心服务

7. 要创建弹性策略，请选择创建策略。

访问弹性策略的详细信息

当您打开弹性策略时，您会看到有关该策略的重要细节。您也可以编辑或删除队列。

弹性策略详细信息包括两个主要视图：摘要和标签。

摘要

基本信息

提供有关弹性策略的以下信息：名称、描述、层级、成本层级和创建日期。

估计工作负载 RTO 和估计工作负载 RPO

显示与此弹性策略相关的估计工作负载 RTO 和估计工作负载 RPO 中断类型。

标签

使用此视图管理、添加和删除此应用程序内部的标签。

在“弹性策略”详细信息中编辑弹性策略

1. 从左侧导航菜单中，选择 Policies (策略)。
2. 在弹性策略中，打开弹性策略。
3. 选择编辑。在基本信息、RTO 和 RPO 字段中输入相应的更改。然后选择 Save changes (保存更改)。

在“弹性策略”中编辑弹性策略

1. 从左侧导航菜单中，选择 Policies (策略)。
2. 在弹性策略中，选择一个弹性策略。
3. 选择 Actions，然后选择 Edit。
4. 在基本信息、RTO 和 RPO 字段中输入相应的更改。然后选择 Save changes (保存更改)。

删除“弹性策略”详细信息中的弹性策略

1. 从左侧导航菜单中，选择 Policies (策略)。

2. 在弹性策略中，打开弹性策略。
3. 选择 Delete (删除)。选择 Delete role (删除角色)，然后确认删除。

删除“弹性策略”中的弹性策略

1. 从左侧导航菜单中，选择 Policies (策略)。
2. 在弹性策略中，选择一个弹性策略。
3. 选择 Actions (操作)，然后选择 Delete (删除)。
4. 选择 Delete role (删除角色)，然后确认删除。

运行和管理 AWS Resilience Hub 弹性评估

当您的应用程序发生更改时，您应该进行弹性评估。评估会将每个应用程序组件配置与策略进行比较，并提出警报、SOP 和测试建议。这些配置建议可以加快恢复过程。

警报建议可帮助您设置用于检测中断的警报。SOP 建议提供了对常见恢复过程（例如从备份中恢复）进行管理的脚本。测试建议提供了验证您的配置是否正常运行的建议。例如，您可以测试应用程序是否在自动恢复过程（例如由于网络问题而导致的自动扩展或负载均衡）中恢复。您可以测试当资源达到限值时是否会触发应用程序警报。您还可以测试 SOP 在您指定的条件下的运作情况。

运行弹性评估

您可以从 AWS Resilience Hub中的多个位置运行弹性评估报告。有关应用程序的更多信息，请参阅 the section called “应用程序”。

从“操作”菜单中运行弹性评估

1. 在左侧的导航菜单中，选择应用程序。
2. 从应用程序表中选择一个应用程序。
3. 从操作菜单中选择评估弹性。
4. 在运行弹性评估对话框中，您可以为评估输入唯一的名称或使用生成的名称。
5. 选择运行。

   要查看评估报告，请在应用程序中选择评估。有关更多信息，请参阅 the section called “查看评估报告”。

从“评估”选项卡中运行弹性评估

当您的应用程序或弹性策略发生更改时，您可以运行新的弹性评估。

1. 在左侧的导航菜单中，选择应用程序。
2. 从应用程序表中选择一个应用程序。
3. 选择评估选项卡。
4. 选择运行弹性评估。
5. 在运行弹性评估对话框中，您可以为评估输入唯一的名称或使用生成的名称。
6. 选择运行。

   要查看评估报告，请在应用程序中选择评估。有关更多信息，请参阅 the section called “查看评估报告”。

查看评估报告

您可以在应用程序的评估视图中找到评估报告。

查找评估报告

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序中，打开一个应用程序。
3. 在评估选项卡中，从弹性评估表中选择评估报告。

打开报告时，可以看到以下内容：

- 评估报告的总体概述
- 提高弹性的建议。
- 设置警报、SOP 和测试的建议
- 如何创建和管理标签以搜索和筛选 AWS 资源

审核

本节概述了评估报告。 AWS Resilience Hub 列出了每种中断类型和相关的应用程序组件。还列出了您的实际 RTO 和 RPO 策略，并确定应用程序组件能否实现策略目标。

概述

显示应用程序的名称、弹性策略的名称以及报告的创建日期。

RTO

以图形方式显示估计应用程序能否达到弹性策略的目标。这是基于在不对组织造成重大损害的情况下可以将应用程序关闭的时间长度。该评估提供了估计的工作负载 RTO。

RPO

以图形方式显示估计应用程序能否达到弹性策略的目标。这是基于在对业务造成重大损害之前数据可能丢失的时间长度。该评估提供了估计的工作负载 RPO。

详细信息

使用所有结果和应用程序合规性偏差选项卡详细描述每种中断类型。所有结果选项卡显示所有中断，包括合规性偏差，而应用程序合规性偏差选项卡仅显示合规性偏差。中断类型包括应用程序、云基础设施（基础设施和可用区）和区域，并提供以下相关信息：

- AppComponent

  构成应用程序的资源。例如，您的应用程序可能具有数据库或计算组件。

- 估计的 RTO

  指示您的策略配置是否符合您的策略要求。我们提供两个值，即我们的估计的 RTO 和您的定向 RTO。例如，如果您在定向 RTO下看到的值为 2h，在估计的工作负载 RTO 下看到的值为 40m，则表示我们提供的估计的工作负载 RTO 为 40 分钟，而您的应用程序的当前 RTO 为两小时。我们的估计的工作负载 RTO 计算是基于配置，而不是策略。因此，无论您选择哪种策略，多可用区数据库在可用区故障时的估计的工作负载 RTO 均相同。

- RTO 偏差

  指示您的应用程序与上一次成功评估的估计的工作负载 RTO 相比的偏差持续时间。我们提供了两个值，即我们的估计的 RTO 和 RTO 偏差。例如，如果您在估计的 RTO 下看到的值为 2h，在 RTO 偏差下看到的值为 40m，则表示您的应用程序与上一次成功评估的估计的工作负载 RTO 之间偏差 40 分钟。

- 估计的 RPO

显示 AWS Resilience Hub 根据您为每个应用程序组件设置的定向 RPO 策略而估算出的实际估计的工作负载 RPO 策略。例如，您可能已在弹性策略中将可用区故障的 RPO 目标设置为一小时。计算出的估计结果可能接近于零。这是假设我们提交每个事务的 Amazon Aurora 在跨越多可用区的六个节点中有四个节点成功完成。 point-in-time 恢复可能需要五分钟。

您唯一可以选择不提供的 RTO 和 RPO 目标是“区域”。对于某些应用程序，当 AWS 服务存在至关重要的依赖项时，对恢复进行计划非常有用，因为该服务可能在整个“区域”不可用。

如果您选择此选项，例如为该“区域”设置 RTO 或 RPO 目标，您将收到此类故障的估计恢复时间和操作建议。

- RPO 偏差

  指示您的应用程序与上一次成功评估的估计的工作负载 RPO 相比的偏差持续时间。我们提供了两个值，即我们的估计的 RPO 和 RPO 偏差。例如，如果您在估计的 RPO 下看到的值为 2h，在 RPO 偏差下看到的值为 40m，则表示您的应用程序与上一次成功评估的估计的工作负载 RPO 之间偏差 40 分钟。

查看弹性建议

弹性建议对应用程序组件进行评估，并根据估计的工作负载 RTO、估计的工作负载 RPO、成本和最小更改来建议如何进行优化。

使用 AWS Resilience Hub，您可以使用 “为什么要选择此选项” 中的以下推荐选项之一来优化弹性：

> **Note**
>
> - AWS Resilience Hub 提供了最多三个 AWS Resilience Hub 推荐选项。
> - 如果您设置了区域 RTO 和 RPO 目标，则会在推荐选项中 AWS Resilience Hub 显示针对区域 RTO/RPO 进行优化。如果未设置区域 RTO 和 RPO 目标，则会显示针对可用区（AZ）RTO/RPO 进行优化。有关在创建弹性策略时设置区域 RTO/RPO 目标的更多信息，请参阅创建弹性策略。
> - 应用程序及其配置的估计工作负载 RTO 和估计的工作负载 RPO 值是通过考虑数据量和个人 AppComponents数据量来确定的。但是，这些数值只是估算值。您应该使用自己的测试（例如 Amazon 错误注入服务）来测试应用程序的实际恢复时间。

针对可用区 RTO/RPO 进行优化

可用区 (AZ) 中断期间可能的最低估计工作负载恢复时间 (RTO/RPO)。如果您的配置更改不足以满足 RTO 和 RPO 目标，则系统会告知您预计的最低工作负载可用区恢复时间，以使您的配置接近达到策略的可能性。

针对区域 RTO/RPO 进行优化

区域性中断期间可能的最低估计工作负载恢复时间 (RTO/RPO)。如果您的配置更改不足以满足 RTO 和 RPO 目标，则系统会告知您预计的最低工作负载区域恢复时间，以使您的配置接近达到策略的可能性。

成本优化

这是您可能产生的最低成本，并且仍然符合您的弹性策略。如果您的配置无法进行充分的更改以实现优化目标，则系统会告知您可以花费的最低成本来使您的配置接近满足策略的可能性。

针对最小更改进行优化

实现政策目标所需的最低限度变动。如果您的配置无法充分更改以满足优化目标，则系统会告知您建议的更改，这些更改可以使您的配置接近满足策略的可能性。

优化类别细分中包括以下项目：

- 描述

  描述建议的配置 AWS Resilience Hub。
- 更改

  描述了切换到建议配置所需任务的文本更改列表。
- 基本成本

  与建议的变更相关的估计成本。

  > **Note**
  >
  > 基本费用可能因使用情况而异，并且不包括企业折扣计划 (EDP) 的任何折扣或优惠。
- 估计的工作负载 RTO 和 RPO

  更改后的估计的工作负载 RTO 和估计的工作负载 RPO。

AWS Resilience Hub 评估应用程序组件 (AppComponent) 是否符合弹性策略。如果 AppComponent 不符合弹性政策，并且 AWS Resilience Hub 无法提出任何促进合规性的建议，则可能是因为在限制范围内 AppComponent 无法满足所选人员的恢复时间。 AppComponent AppComponent 限制的示例包括资源类型、存储大小或资源配置。

为便于遵守弹性政策，请更改弹性策略的资源类型 AppComponent 或更新弹性策略，使其与资源所能提供的内容保持一致。 AppComponent

审查操作建议

操作建议包含通过 AWS CloudFormation 模板设置警报、SOP 和 AWS FIS 实验的建议。

AWS Resilience Hub 提供 AWS CloudFormation 模板文件供您下载并以代码形式管理应用程序的基础架构。因此，我们在 AWS CloudFormation 中提供了建议，以便您可以将其添加到应用程序代码中。如果 AWS CloudFormation 模板文件的大小超过 1 MB 且包含的资源超过 500 个，则 AWS Resilience Hub 会生成多个 AWS CloudFormation 模板文件，其中每个文件的大小不超过 1 MB，最多包含 500 个资源。如果将 AWS CloudFormation 模板文件拆分为多个文件，则 AWS CloudFormation 模板文件名将附加在后面`partXofY`，其中`X`表示序列中的文件号，并`Y`表示 AWS CloudFormation 模板文件被分成的文件总数。例如，如果将模板文件 `big-app-template5-Alarm-104849185070-us-west-2.yaml` 分为四个文件，则文件名将如下所示：

- `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`

但是，对于大型 AWS CloudFormation 模板，您需要提供亚马逊简单存储服务 URI，而不是使用本地文件作为输入的 CLI/API。

在中 AWS Resilience Hub，您可以执行以下操作：

- 您可以配置选定的警报、SOP 和 AWS FIS 实验。要配置警报、SOP 和 AWS FIS 实验，请选择相应的建议并输入唯一的名称。 AWS Resilience Hub 根据您选择的推荐创建模板。在模板中，您可以通过 Amazon Simple Storage Service（Amazon S3）URL 访问您创建的模板。
- 您可以包括或排除在任何时间点为您的应用程序推荐的选定警报、SOP 和 AWS FIS 实验。有关更多信息，请参阅the section called “包含或排除操作建议”。
- 您还可以搜索、创建、添加、移除和管理应用程序的标签，并查看与应用程序关联的所有标签。

包含或排除操作建议

AWS Resilience Hub 提供了一个选项，用于包括或排除为提高应用程序在任何时间点的弹性分数而推荐的警报、SOP 和 AWS FIS 实验（测试）。只有在您进行新的评估后，包含和排除操作建议才会对应用程序的弹性得分产生影响。因此，我们建议您进行评估，以获取更新的弹性分数，并了解其对应用程序的影响。

有关对每个应用程序包含或排除建议的权限进行限制的更多信息，请参阅 the section called “限制包含或排除 AWS Resilience Hub 建议的权限”。

在应用程序中包含或排除操作建议

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序中，打开一个应用程序。
3. 选择评估，然后从弹性评估表中选择一项评估。如果您没有进行评估，请完成 the section called “运行弹性评估” 中的过程，然后返回此步骤。
4. 选择操作建议选项卡。
5. 要在应用程序中包含或排除操作建议，请完成以下过程：

在应用程序中包含或排除建议的警报

1. 要排除警报，请完成以下步骤：
    a. 在警报选项卡下，从警报表中选择要排除的所有警报（处于未实施状态）。您可以从状态列中识别警报的当前实施状态。
    b. 从操作中选择排除选定项。
    c. 从排除建议对话框中，选择以下原因之一（可选），然后选择排除选定项，将所选警报从应用程序中排除。
        - 已实施 — 如果您已经在诸如Amazon或任何其他第三方服务提供商之类的 AWS 服务中实施了这些警报 CloudWatch，请选择此选项。
        - 不相关 — 如果警报不符合您的业务需求，请选择此选项。
        - 实施起来太复杂 — 如果您认为这些警报太复杂而无法实施，请选择此选项。
        - 其他 — 选择此选项以指明排除该建议的任何其他原因。
2. 要包含警报，请完成以下步骤：

a. 在警报选项卡下，从警报表中选择要包含的所有警报（处于已排除状态）。您可以从状态列中识别警报的当前实施状态。

b. 从操作中选择包含选定项。

c. 从包含建议对话框中，选择包含选定项，将所有选定的警报都包含在应用程序中。

在应用程序中包含或排除建议的标准操作流程（SOP）

1. 要排除建议的 SOP，请完成以下步骤：

   a. 在标准操作流程选项卡下，从 SOP 表中选择要排除的所有 SOP（处于已实施或未实施状态）。您可以从状态列中识别 SOP 的当前实施状态。

   b. 在操作中，选择排除选定项，将选定的 SOP 从您的应用程序中排除。

   c. 从排除建议对话框中，选择以下原因之一（可选），然后选择排除选定项，将选定的 SOP 从应用程序中排除。

      - 已经实施 — 如果您已经在 AWS 服务或任何其他第三方服务提供商中实施了这些 SOP，请选择此选项。
      - 不相关 — 如果 SOP 不符合您的业务需求，请选择此选项。
      - 实施起来太复杂 — 如果您认为这些 SOP 太复杂而无法实施，请选择此选项。
      - 无 — 如果您不想指明原因，请选择此选项。

2. 要包含 SOP，请完成以下步骤：

   a. 在标准操作流程选项卡下，从 SOP 表中选择要包含的所有警报（处于已排除状态）。您可以从状态列中识别警报的当前实施状态。

   b. 从操作中选择包含选定项。

   c. 从包含建议对话框中，选择包含选定项，将所有选定的 SOP 包含在应用程序中。

在应用程序中包含或排除建议的测试

1. 要排除建议的测试，请完成以下步骤：

   a. 在错误注入实验模板选项卡下，从错误注入实验模板表中，选择要排除的所有测试（处于已实施或未实施状态）。您可以从状态列中识别测试的当前实施状态。

   b. 从操作中选择排除选定项。

c. 从排除建议对话框中，选择以下原因之一（可选），然后选择排除选定项，将选定的 AWS FIS 实验从应用程序中排除。

- 已实施 — 如果您已经在服务或任何其他第三方 AWS 服务提供商中实施了这些测试，请选择此选项。
- 不相关 — 如果测试不符合您的业务需求，请选择此选项。
- 实施起来太复杂 — 如果您认为这些测试太复杂而无法实施，请选择此选项。
- 无 — 如果您不想指明原因，请选择此选项。

2. 要包含建议的测试，请完成以下步骤：

a. 在错误注入实验模板选项卡下，从错误注入实验模板表中选择要包含的所有测试（处于已排除状态）。您可以从状态列中识别测试的当前实施状态。

b. 从操作中选择包含选定项。

c. 从包括建议对话框中，选择包含选定项，将所有选定的测试都包含在应用程序中。

删除弹性评估

您可以在应用程序的评估视图中删除弹性评估。

删除弹性评估

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序中，打开一个应用程序。
3. 在评估中，选择弹性评估表中的评估报告。
4. 要确认删除，请选择删除。

该报告不再出现在弹性评估表中。

管理警报

在运行弹性评估时，作为操作建议的一部分， AWS Resilience Hub 建议设置 Amazon CloudWatch 警报以监控您的应用程序弹性。这些警报建议是基于您当前应用程序配置的资源和组件。如果应用程序中的资源和组件发生变化，则应运行弹性评估，以确保更新后的应用程序收到正确的警报。

AWS Resilience Hub 提供了一个模板文件 (README.md)，允许您创建 AWS Resilience Hub 内部 AWS （例如 Amazon CloudWatch）或外部推荐的警报 AWS。警报中提供的默认值基于创建这些警报时使用的最佳实践。

主题

根据操作建议创建警报

AWS Resilience Hub 创建包含在 Amazon 中创建所选警报的详细信息的 AWS CloudFormation 模板 CloudWatch。生成模板后，您可以通过 Amazon S3 URL 访问该模板，下载该模板并将其放入您的代码管道中，或者通过 AWS CloudFormation 控制台创建堆栈。

要根据 AWS Resilience Hub 建议创建警报，必须为推荐的警报创建 AWS CloudFormation 模板并将其包含在代码库中。

在操作建议中创建警报

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序中，选择您的应用程序。
3. 选择评估选项卡。

   在弹性评估表中，您可以使用以下信息来标识您的评估：

   - 名称 — 创建评估时提供的评估名称。
   - 状态 — 指示评估的实施状态。
   - 合规性状态 — 指示评估是否符合弹性策略。
   - 弹性偏差状态 — 指示您的应用程序是否与之前的成功评估有所偏差。
   - 应用程序版本 — 应用程序的版本。
   - 调用者 — 指示调用评估的角色。
   - 开始时间 — 表示评估的开始时间。
   - 结束时间 — 表示评估的结束时间。
   - ARN — 评估的 Amazon 资源名称（ARN）。
4. 从弹性评估表中选择一项评估。如果您没有进行评估，请完成 the section called “运行弹性评估” 中的过程，然后返回此步骤。

5. 选择操作建议。
6. 如果默认情况下未选中，请选择警报选项卡。

   在警报表中，您可以使用以下方式标识建议的警报：

   - 名称 — 您为应用程序设置的警报的名称。
   - 描述 — 描述警报的目标。
   - 状态 — 表示 Amazon CloudWatch 警报的当前实施状态。

     该列显示以下值之一：

     - 已实施-表示建议的警报已 AWS Resilience Hub 在您的应用程序中实现。选择下面的数字可对警报表进行筛选，以显示您的应用程序中实施的所有建议警报。
     - 未实现 — 表示您的应用程序中包含 AWS Resilience Hub 但未实现推荐的警报。选择下面的数字可对警报表进行筛选，以显示您的应用程序中未实施的所有建议警报。
     - 已@@ 排除-表示您的应用程序中 AWS Resilience Hub 已排除推荐的警报。选择下面的数字可对警报表进行筛选，以显示从您的应用程序中排除的所有建议警报。有关包含和排除建议警报的更多信息，请参阅包含或排除操作建议。
     - 非活动 — 表示警报已部署到亚马逊 CloudWatch，但亚马逊中的状态设置为 INSUFKIENT_DATA。 CloudWatch选择下面的数字可对警报表进行筛选，以显示所有已实施但非活动的警报。
   - 配置 — 指示是否有任何待处理的配置依赖项需要解决。
   - 类型 — 表示警报的类型。
   - AppComponent— 表示与此警报关联的应用程序组件 (AppComponents)。
   - 引用 ID — 表示中 AWS CloudFormation 堆栈事件的逻辑标识符 AWS CloudFormation。
   - 建议 ID — 表示中 AWS CloudFormation 堆栈资源的逻辑标识符 AWS CloudFormation。
7. 在警报选项卡中，如要根据特定状态筛选警报表中的警报建议，请在该状态下选择一个数字。
8. 选择要为应用程序设置的推荐警报，然后选择创建 CloudFormation 模板。
9. 在 “创建 CloudFormation 模板” 对话框中，您可以使用自动生成的名称，也可以在 AWS CloudFormation 模板名称框中输入CloudFormation 模板的名称。
10. 选择创建。创建 AWS CloudFormation 模板可能需要几分钟。

    完成以下过程以将建议包含在代码库中。

要在代码库中加入 AWS Resilience Hub 建议

1. 选择模板选项卡以查看刚才创建的模板。您可以使用以下方式来标识模板：
   - 名称 — 创建评估时提供的评估名称。
   - 状态 — 指示评估的实施状态。
   - 类型 — 表示操作建议的类型。
   - 格式 — 表示创建模板的格式（JSON/文本）。
   - 开始时间 — 表示评估的开始时间。
   - 结束时间 — 表示评估的结束时间。
   - ARN — 模板的 ARN
2. 在模板详细信息下，选择模板 S3 路径下方的链接，在 Amazon S3 控制台中打开模板对象。
3. 在 Amazon S3 控制台中，从对象表中选择 SOP 文件夹链接。
4. 要复制 Amazon S3 路径，请选中 JSON 文件前面的复选框并选择复制 URL。
5. 从 AWS CloudFormation 控制台创建 AWS CloudFormation 堆栈。有关创建 AWS CloudFormation 堆栈的更多信息，请参阅https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html。

   创建 AWS CloudFormation 堆栈时，必须提供从上一步中复制的 Amazon S3 路径。

查看警报

您可以查看为监控应用程序弹性而设置的所有活动警报。 AWS Resilience Hub 使用 AWS CloudFormation 模板存储警报详情，这些详细信息反过来又用于在 Amazon CloudWatch 中创建警报。您可以使用 Amazon S3 URL 访问 AWS CloudFormation 模板，也可以将其下载并放入您的代码管道或通过 AWS CloudFormation 控制台创建堆栈。

要从控制面板查看警报，请从左侧导航菜单中选择控制面板。在警报表中，您可以使用以下信息标识已实施的警报：

- 受到影响的应用程序 — 已实施此警报的应用程序的名称。
- 活动警报 — 表示应用程序触发的活动警报数量。
- FIS 正在进行中 — 表示当前正在为您的应用程序运行的 AWS FIS 实验。

查看应用程序中已实施的警报

1. 在左侧的导航菜单中，选择应用程序。
2. 从应用程序表中选择一个应用程序。
3. 在应用程序摘要页面中，已实施的警报表显示了在您的应用程序中实施的所有建议警报。

   要在已实施的警报表中查找特定警报，请在按文本、属性或值查找警报框中，选择以下字段之一，选择一个操作，然后键入一个值。

   - 警报名称 — 您为应用程序设置的警报的名称。
   - 描述 — 描述警报的目标。
   - 状态 — 表示 Amazon CloudWatch 警报的当前实施状态。

     该列显示以下值之一：

     - 已实施-表示建议的警报已 AWS Resilience Hub 在您的应用程序中实现。选择下面的数字，在操作建议选项卡中查看所有建议和已实施的警报。
     - 未实现 — 表示您的应用程序中包含 AWS Resilience Hub 但未实现推荐的警报。选择下面的数字，在操作建议选项卡中查看所有建议但未实施的警报。
     - 已@@ 排除-表示您的应用程序中 AWS Resilience Hub 已排除推荐的警报。选择下面的数字，在操作建议选项卡中查看所有建议但已排除的警报。有关包含和排除建议警报的更多信息，请参阅包含或排除操作建议。
     - 非活动 — 表示警报已部署到亚马逊 CloudWatch，但亚马逊中的状态设置为 INSUFKIENT_DATA。 CloudWatch选择下面的数字，在操作建议选项卡中查看所有已实施但非活动的警报。
   - 源模板-提供包含警报详细信息的 AWS CloudFormation 堆栈的 Amazon 资源名称 (ARN)。
   - 资源 — 显示警报附加到的资源以及实施警报所用的资源。
   - 指标-显示为警报分配的 Amazon CloudWatch 指标。有关亚马逊 CloudWatch 指标的更多信息，请参阅亚马逊 CloudWatch 指标。
   - 上一次更改 — 显示上一次修改警报的日期和时间。

从评估中查看建议的警报

1. 在左侧的导航菜单中，选择应用程序。
2. 从应用程序表中选择一个应用程序。

   要查找应用程序，请在查找应用程序框中输入应用程序名称。

3. 选择评估选项卡。

   在弹性评估表中，您可以使用以下信息来标识您的评估：

   - 名称 — 创建评估时提供的评估名称。
   - 状态 — 指示评估的实施状态。
   - 合规性状态 — 指示评估是否符合弹性策略。
   - 弹性偏差状态 — 指示您的应用程序是否与之前的成功评估有所偏差。
   - 应用程序版本 — 应用程序的版本。
   - 调用者 — 指示调用评估的角色。
   - 开始时间 — 表示评估的开始时间。
   - 结束时间 — 表示评估的结束时间。
   - ARN — 评估的 Amazon 资源名称（ARN）。
4. 从弹性评估表中选择一项评估。
5. 选择操作建议选项卡。
6. 如果默认情况下未选中，请选择警报选项卡。

   在警报表中，您可以使用以下方式标识建议的警报：

   - 名称 — 您为应用程序设置的警报的名称。
   - 描述 — 描述警报的目标。
   - 状态 — 表示 Amazon CloudWatch 警报的当前实施状态。

     该列显示以下值之一：

     - 已实施 — 表示警报已在您的应用程序中实施。选择下面的数字可对警报表进行筛选，以显示您的应用程序中实施的所有建议警报。
     - 未实施 — 表示警报未在您的应用程序中实施或未包含在内。选择下面的数字可对警报表进行筛选，以显示您的应用程序中未实施的所有建议警报。
     - 已排除 — 表示警报已从应用程序中排除。选择下面的数字可对警报表进行筛选，以显示从您的应用程序中排除的所有建议警报。有关包含和排除建议警报的更多信息，请参阅 the section called “包含或排除操作建议”。
     - 非活动 — 表示警报已部署到亚马逊 CloudWatch，但亚马逊中的状态设置为 INSUFKIENT_DATA。 CloudWatch选择下面的数字可对警报表进行筛选，以显示所有已实施但非活动的警报。
   - 配置 — 指示是否有任何待处理的配置依赖项需要解决。

- 类型 — 表示警报的类型。
- AppComponent— 表示与此警报关联的应用程序组件 (AppComponents)。
- 引用 ID — 表示中 AWS CloudFormation 堆栈事件的逻辑标识符 AWS CloudFormation。
- 建议 ID — 表示中 AWS CloudFormation 堆栈资源的逻辑标识符 AWS CloudFormation。

标准操作流程

标准操作流程 (SOP) 是一套规范性步骤，旨在在出现中断或警报时有效地恢复应用程序。对您的 SOP 进行提前构建、测试和衡量，以确保在出现运行中断时及时恢复。

根据您的应用程序组件，AWS Resilience Hub 为您建议了应构建的 SOP。AWS Resilience Hub 与 Systems Manager 合作，提供了大量的 SSM 文档，可用作您的 SOP 的构建依据，使 SOP 构建步骤自动化。

例如，AWS Resilience Hub 可能会根据现有的 SSM 自动化文档推荐用于添加磁盘空间的 SOP。要运行此 SSM 文档，您需要具有正确权限的特定 IAM 角色。AWS Resilience Hub 在您的应用程序中创建元数据，指明在磁盘空间不足的情况下要运行哪个 SSM 自动化文档，以及需要何种 IAM 角色才能运行该 SSM 文档。然后将此元数据保存在 SSM 参数中。

除了配置 SSM 自动化之外，最好的做法是通过 AWS FIS 实验对其进行测试。因此，AWS Resilience Hub 还提供了一个调用 SSM 自动化文档的 AWS FIS 实验。通过这种方式，您可以主动测试您的应用程序，以确保您创建的 SOP 能完成预期的工作。

AWS Resilience Hub 采用 AWS CloudFormation 模板的形式提供其建议，您可以将其添加到应用程序代码库中。此模板提供：

- 运行 SOP 所需权限的 IAM 角色。
- 您可以用来测试 SOP 的 AWS FIS 实验。
- 一个包含应用程序元数据的 SSM 参数，指出哪个 SSM 文档和何种 IAM 角色将作为 SOP 运行，以及在哪个资源上运行。例如：`$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`。

创建 SOP 可能需要反复试验。对您的应用程序进行弹性评估并根据 AWS Resilience Hub 建议生成 AWS CloudFormation 模板是个不错的开始。使用 AWS CloudFormation 模板生成 AWS CloudFormation 堆栈，然后在 SOP 中使用 SSM 参数及其默认值。运行 SOP，以查看需要进行哪些改进。

由于所有应用程序都有不同的要求，因此 AWS Resilience Hub 提供的默认 SSM 文档列表不足以满足您的所有需求。但是，您可以复制默认 SSM 文档，并以它们为依据创建专为您的应用程序量身定制的自定义文档。您还可以创建自己的全新 SSM 文档。如果您创建自己的 SSM 文档而不是修改默认值，则必须将它们与 SSM 参数相关联，这样在 SOP 运行时就会调用正确的 SSM 文档。

通过创建必要的 SSM 文档并根据需要更新参数和文档之间的关联，从而最终确定 SOP 后，请将 SSM 文档直接添加到您的代码库中，并在库中进行任何后续更改或自定义。这样，每次部署应用程序时，您还将部署最新的 SOP。

主题

根据 AWS Resilience Hub 建议构建 SOP

要根据 AWS Resilience Hub 建议构建 SOP，您需要一个附加有弹性策略的 AWS Resilience Hub 应用程序，并且需要对该应用程序进行弹性评估。弹性评估会为您的 SOP 生成建议。

要根据 AWS Resilience Hub 建议构建 SOP，您必须为建议的 SOP 创建 AWS CloudFormation 模板并将其包含在代码库中。

为 SOP 建议创建 AWS CloudFormation 模板

1. 打开 AWS Resilience Hub 控制台。
2. 在导航窗格中，选择 Applications（应用程序）。
3. 从应用程序列表中，选择要创建 SOP 的应用程序。
4. 选择评估选项卡。
5. 从弹性评估表中选择一项评估。如果您没有进行评估，请完成 the section called “运行弹性评估” 中的过程，然后返回此步骤。
6. 在操作建议下，选择标准操作流程。
7. 选择您要包含的所有 SOP 建议。
8. 选择创建 CloudFormation 模板。创建 AWS CloudFormation 模板可能需要几分钟时间。

完成以下过程以将 SOP 建议包含在代码库中。

将 AWS Resilience Hub 建议包含在代码库中

1. 在操作建议中，选择模板。
2. 在模板列表中，选择刚才创建的 SOP 模板的名称。

   您可以使用以下信息来标识应用程序中实施的 SOP：

   - SOP 名称 — 您为应用程序指定的 SOP 的名称。
   - 描述 — 描述 SOP 的目标。
   - SSM 文档 — 包含 SOP 定义的 SSM 文档的 Amazon S3 URL。
   - 测试运行 — 包含最新测试结果的文档的 Amazon S3 URL。
   - 源模板 — 提供包含 SOP 详细信息的 AWS CloudFormation 堆栈的 Amazon 资源名称 (ARN)。
3. 在模板详细信息下，选择模板 S3 路径中的链接，在 Amazon S3 控制台中打开模板对象。
4. 在 Amazon S3 控制台中，从对象表中选择 SOP 文件夹链接。
5. 要复制 Amazon S3 路径，请选中 JSON 文件前面的复选框并选择复制 URL。
6. 在 AWS CloudFormation 控制台中创建 AWS CloudFormation 堆栈。有关创建 AWS CloudFormation 堆栈的更多信息，请参阅 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html。

   创建 AWS CloudFormation 堆栈时，必须提供从上一步中复制的 Amazon S3 路径。

删除自定义 SSM 文档

要完全自动恢复应用程序，您可能需要在 Systems Manager 控制台中为 SOP 创建自定义 SSM 文档。您可以将现有的 SSM 文档作为基础进行修改，也可以创建新的 SSM 文档。

有关使用 Systems Manager 创建 SSM 文档的详细信息，请参阅演练：使用文档生成器创建自定义运行手册。

有关 SSM 文档语法的信息，请参阅 SSM 文档语法。

有关 SSM 自动化文档操作的更多信息，请参阅Systems Manager 自动化操作参考。

使用自定义 SSM 文档而不是默认的 SSM 文档

要将 AWS Resilience Hub 为您的 SOP 建议的 SSM 文档替换为您创建的自定义文档，请直接在代码库中操作。除了添加新的自定义 SSM 自动化文档外，您还将：

1. 添加运行自动化所需的 IAM 权限。
2. 添加 AWS FIS 实验来测试您的 SSM 文档。
3. 添加一个 SSM 参数，该参数指向要用作 SOP 的自动化文档。

通常，使用 AWS Resilience Hub 中建议的默认值并根据需要对其进行自定义，这样的效率最高。例如，根据需要为 IAM 角色添加或删除权限，将 AWS FIS 实验设置更改为指向新的 SSM 文档，或者更改 SSM 参数以指向您的新 SSM 文档。

测试 SOP

如前所述，最佳做法是在 CI/CD 管道中添加 AWS FIS 实验，以定期测试 SOP；这样可以确保在发生中断时随时可以启动 SOP。

测试 AWS Resilience Hub 提供的 SOP 和自定义 SOP。

查看标准操作流程

查看应用程序中已实施的 SOP

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序中，打开一个应用程序。
3. 选择标准操作流程选项卡。

   在标准操作流程摘要章节中，已实施的标准操作流程表中显示了根据 SOP 建议生成的 SOP 列表。

   您可以通过以下方式标识您的 SOP：

   - SOP 名称 — 您为应用程序指定的 SOP 的名称。
   - SSM 文档 — 包含 SOP 定义的 Amazon EC2 Systems Manager 文档的 S3 URL。
   - 描述 — 描述 SOP 的目标。
   - 测试运行 — 包含最新测试结果的文档的 S3 URL。
   - 参考 ID — 所引用的 SOP 建议的标识符。

- 资源 ID — 实施 SOP 建议的资源的标识符。

查看评估建议的 SOP

1. 在左侧的导航菜单中，选择应用程序。
2. 从应用程序表中选择一个应用程序。

   要查找应用程序，请在查找应用程序框中输入应用程序名称。
3. 选择评估选项卡。

   在弹性评估表中，您可以使用以下信息来标识您的评估：

   - 名称 — 创建评估时提供的评估名称。
   - 状态 — 指示评估的实施状态。
   - 合规性状态 — 指示评估是否符合弹性策略。
   - 弹性偏差状态 — 指示您的应用程序是否与之前的成功评估有所偏差。
   - 应用程序版本 — 应用程序的版本。
   - 调用者 — 指示调用评估的角色。
   - 开始时间 — 表示评估的开始时间。
   - 结束时间 — 表示评估的结束时间。
   - ARN — 评估的 Amazon 资源名称（ARN）。
4. 从弹性评估表中选择一项评估。
5. 选择操作建议选项卡。
6. 选择标准操作流程选项卡。

   在标准操作流程表中，您可以使用以下信息进一步了解建议的 SOP：

   - 名称 — 建议的 SOP 的名称。
   - 描述 — 描述 SOP 的目标。
   - 状态 — 表示 SOP 的当前实施状态。即已实施、未实施和已排除。
   - 配置 — 指示是否有任何待处理的配置依赖项需要解决。
   - 类型 — 表示 SOP 的类型。
   - AppComponent — 表示与此 SOP 关联的应用程序组件 (AppComponents)。有关支持的 AppComponents 的更多信息，请参阅在 AppComponent 中对资源进行分组。

- 参考 ID — 表示 AWS CloudFormation 中 AWS CloudFormation 堆栈事件的逻辑标识符。
- 建议 ID — 表示 AWS CloudFormation 中 AWS CloudFormation 堆栈资源的逻辑标识符。

Amazon 错误注入服务实验

本节介绍如何在 AWS Resilience Hub中创建和运行 Amazon 错误注入服务（AWS FIS）实验。您可以通过 AWS FIS 实验来衡量 AWS 资源的弹性以及从应用程序、基础架构、可用区和 AWS 区域 事件中恢复所需的时间。

为了衡量弹性，这些 AWS FIS 实验模拟了您的 AWS 资源中断。中断的示例包括网络不可用错误、故障转移、Amazon EC2 或 AWS ASG 上的进程停止、Amazon RDS 中的启动恢复以及可用区域的问题。 AWS FIS 实验结束后，您可以估计应用程序能否从弹性策略的 RTO 目标中定义的中断类型中恢复。

中的所有实验 AWS Resilience Hub 都是使用构建的 AWS FIS ，它们可以执行 AWS FIS 动作。大多数 AWS FIS 实验调用 Systems Manager 自动化操作来执行中断和监控警报，而其他 AWS FIS 实验仅使用针对特定 AWS 服务定制的 AWS FIS 自动化操作（例如 Amazon EKS 操作）。有关 AWS FIS 操作的更多信息，请参阅 AWS FIS 规则参考。

您可以在 AWS FIS 实验的默认状态下使用它们，也可以根据自己的要求对其进行自定义。 AWS FIS 可以从 AWS Resilience Hub (the section called “查看错误注入实验”) 或 AWS FIS 控制台 (AWS FIS) 访问实验。

主题

- 根据操作建议创建 AWS FIS 实验
- 从中运行 AWS FIS 实验 AWS Resilience Hub
- 查看错误注入实验
- Amazon 错误注入服务实验失败/状态检查

根据操作建议创建 AWS FIS 实验

AWS Resilience Hub 建议您在运行评估报告后测试应用程序。您可以从应用程序的评估报告中访问和运行这些实验。

AWS Resilience Hub 提供了实验列表，这些 AWS FIS 实验是带有测试参数的 Systems Manager 文档。当您从列表中选择 AWS FIS 实验时， AWS Resilience Hub 会使用您在 Systems Manager 文档

中定义的参数创建一个 AWS CloudFormation 模板。创建 AWS CloudFormation 堆栈后，您可以看到为应用程序预配置的 AWS FIS 实验。

该 AWS CloudFormation 模板由每个 Systems Manager 文档的 IAM 角色组成，该角色具有运行所需的最低权限。

要根据 AWS Resilience Hub 建议创建 AWS FIS 实验，必须为推荐的测试创建 AWS CloudFormation 模板并将其包含在代码库中。

为 AWS FIS 实验创建 AWS CloudFormation 模板

1. 打开控制 AWS Resilience Hub 台。
2. 在导航窗格中，选择 应用程序。
3. 从应用程序列表中，选择要为其创建测试的应用程序。
4. 选择评估选项卡。
5. 从弹性评估表中选择一项评估。如果您没有进行评估，请完成 the section called “运行弹性评估” 中的过程，然后返回此步骤。
6. 在操作建议下，选择错误注入实验。
7. 选择要包含的所有测试。
8. 选择创建 CloudFormation 模板。创建 AWS CloudFormation 模板可能需要几分钟。
9. 选择 模板。

   您可以在 “模板” 表格中查看新创建的 AWS CloudFormation 模板。

   完成以下过程以将建议包含在代码库中。

在代码库中加入 AWS Resilience Hub 建议

1. 在操作建议中，选择模板。
2. 在模板列表中，选择您刚刚创建的 AWS FIS 实验模板的名称。

   您可以使用以下信息来标识应用程序中实施的测试：

   - 测试名称 — 您为应用程序创建的测试的名称。
   - 描述 — 描述测试的目标。
   - 状态 — 表示测试的当前实施状态。

     该列显示以下值之一：

- 已实施 — 表示您的应用程序中已实施该测试。
- 未实施 — 表示您的应用程序中未实施或未包含该测试。
- 已排除 — 表示该测试已从应用程序中排除。
- 非活动 — 表示测试已部署到 AWS FIS，但在过去 30 天内未运行。

- 测试运行 — 包含最新测试结果的文档的 Amazon S3 URL。
- 源模板-提供包含实验详细信息的 AWS CloudFormation 堆栈的 Amazon 资源名称 (ARN)。

3. 在模板详细信息下，选择模板 S3 路径中的链接，在 Amazon S3 控制台中打开模板对象。
4. 在 Amazon S3 控制台中，从对象表中选择测试文件夹链接。
5. 要复制 Amazon S3 路径，请选中 JSON 文件前面的复选框并选择复制 URL。
6. 从 AWS CloudFormation 控制台创建 AWS CloudFormation 堆栈。有关创建 AWS CloudFormation 堆栈的更多信息，请参阅https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html。

   创建 AWS CloudFormation 堆栈时，必须提供从上一步中复制的 Amazon S3 路径。

从中运行 AWS FIS 实验 AWS Resilience Hub

在您的应用程序中，必须先根据操作建议创建 AWS FIS 实验模板，然后 AWS Resilience Hub 才能运行 AWS FIS 实验。

开始实 AWS FIS 验

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序表中，打开一个应用程序。
3. 选择错误注入实验选项卡。
4. 从实验模板表中选择用于创建要运行的实验的实验模板前面的单选按钮，然后选择开始实验。

停止实 AWS FIS 验

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序表中，打开一个应用程序。
3. 选择错误注入实验选项卡。
4. 从实验表中选择实验前面的单选按钮，然后选择停止实验。

查看错误注入实验

在中 AWS Resilience Hub，查看您为衡量 AWS 资源的弹性以及从应用程序、基础架构、可用区和 AWS 区域 事件中恢复所需的时间而设置的 AWS FIS 实验。

要从仪表板查看 AWS FIS 实验，请从左侧导航菜单中选择 “仪表板”。在 “实验” 表中，您可以使用以下信息识别已实现的 AWS FIS 实验：

- 实验 ID — AWS FIS 实验的标识符。
- 实验模板 ID — 用于创建 AWS FIS 实验的实验模板的标识符。 AWS FIS
- 源模板-提供包含实验详细信息的 AWS CloudFormation 堆栈的 Amazon 资源名称 (ARN)。 AWS FIS
- 状态-指示 AWS FIS 实验是否成功完成。

从应用程序中查看已实现的 AWS FIS 实验

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序表中，打开一个应用程序。
3. 选择错误注入实验。
4. 选择实验选项卡。

   在 “实验” 选项卡中，您可以在 “ AWS FIS 实验” 表中看到正在进行的实验列表。

   在实验表中，您可以使用以下信息标识已实施的 AWS FIS 实验：

   - 测试名称 — 用于创建 AWS FIS 实验的 AWS Resilience Hub 推荐测试的名称。
   - 实验 ID — AWS FIS 实验的标识符。
   - 描述-描述 AWS FIS 实验的目标。
   - 创建时间 — 创建 AWS FIS 实验的日期和时间。
   - 上次更新时间 — AWS FIS 实验上次更新的日期和时间。
   - 源模板-提供包含实验详细信息的 AWS CloudFormation 堆栈的 Amazon 资源名称 (ARN)。 AWS FIS

查看评估中建议的实验

1. 在左侧的导航菜单中，选择应用程序。

2. 从应用程序表中选择一个应用程序。

   要查找应用程序，请在查找应用程序框中输入应用程序名称。

3. 选择评估选项卡。

   在弹性评估表中，您可以使用以下信息来标识您的评估：

   - 名称 — 创建评估时提供的评估名称。
   - 状态 — 指示评估的实施状态。
   - 合规性状态 — 指示评估是否符合弹性策略。
   - 弹性偏差状态 — 指示您的应用程序是否与之前的成功评估有所偏差。
   - 应用程序版本 — 应用程序的版本。
   - 调用者 — 指示调用评估的角色。
   - 开始时间 — 表示评估的开始时间。
   - 结束时间 — 表示评估的结束时间。
   - ARN — 评估的 Amazon 资源名称（ARN）。

4. 从弹性评估表中选择一项评估。
5. 选择操作建议选项卡。
6. 选择错误注入实验选项卡。

   在错误注入实验模板表中，您可以使用以下信息进一步了解建议的测试：

   - 名称 — 建议的测试的名称。
   - 描述 — 描述测试的目标。
   - 状态 — 表示测试的当前实施状态。

     该列显示以下值之一：

     - 已实施 — 表示您的应用程序中已实施该测试。
     - 未实施 — 表示您的应用程序中未实施或未包含该测试。
     - 已排除 — 表示该测试已从应用程序中排除。
     - 非活动 — 表示测试已部署到 AWS FIS，但在过去 30 天内未运行。

   - 配置 — 指示是否有任何待处理的配置依赖项需要解决。
   - 类型 — 表示测试的类型。

- AppComponent— 表示与此测试关联的应用程序组件 (AppComponents)。有关支持的更多信息 AppComponents，请参阅中对资源进行分组 AppComponent。
- 风险 — 表示测试失败的风险等级。使用高、中和低来分别表示高、中和低风险等级。
- 参考 ID — 表示中 AWS CloudFormation 堆栈事件的逻辑标识符 AWS CloudFormation。
- 建议 ID — 表示中 AWS CloudFormation 堆栈资源的逻辑标识符 AWS CloudFormation。

Amazon 错误注入服务实验失败/状态检查

AWS Resilience Hub 允许您跟踪已开始的实验的状态。有关更多信息，请参阅 the section called “查看错误注入实验” 中的查看评估中建议的实验中的程序。

主题

- 使用 S AWS ystems Manager 分析 AWS FIS 实验执行情况
- AWS FIS 测试在亚马逊 Elastic Kubernetes Service 集群中运行的 Kubernetes 容器时实验失败

使用 S AWS ystems Manager 分析 AWS FIS 实验执行情况

运行 AWS FIS 实验后，您可以在 S AWS ystems Manager 中查看执行细节。

1. 前往 CloudTrail> 事件历史记录。
2. 使用实验 ID 按用户名筛选事件。
3. 查看条 StartAutomationExecution 目。请求 ID 是 SSM 自动化 ID。
4. 前往 AWS Systems Manager > 自动化。
5. 使用 SSM 自动化 ID 按执行 ID 筛选并查看自动化详细信息。

   您可以使用任何 Systems Manager 自动化来分析执行情况。有关更多信息，请参阅 AWS Systems Manager Automation 用户指南。执行输入参数显示在执行详细信息的 “输入参数” 部分，包括 AWS FIS 实验中未出现的可选参数。

   通过深入了解执行步骤中的具体步骤，可以找到有关步骤状态和其他步骤详情的信息。

常见失败情况

以下是在执行评估报告时遇到的常见失败情况：

- 在执行测试/SOP 实验之前，未部署警报模板。这会导致在自动化步骤中出现错误消息。

  - 失败消息：`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.`
  - 补救措施：在重新运行错误注入实验之前，请确保呈现相关警报并部署生成的模板。
- 执行角色缺少权限。如果提供的执行角色缺少权限并出现在步骤详情中，则会出现此错误消息。
  - 失败消息：`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。`
  - 补救措施：验证您提供的执行角色是否正确。如果已完成此操作，请添加所需的权限并重新运行评估。
- 执行成功但没有得到预期的结果。这是由于参数不正确或内部自动化问题造成。
  - 失败消息：执行成功，因此未显示任何错误消息。
  - 补救：在检查预期输入和输出的各个步骤之前，请检查输入参数并查看已执行的步骤，如分析 AWS FIS 实验执行中所述。

AWS FIS 测试在亚马逊 Elastic Kubernetes Service 集群中运行的 Kubernetes 容器时实验失败

以下是在对 Amazon EKS 集群中运行的 Kubernetes 容器组（pod）进行测试时遇到的常见 Amazon Elastic Kubernetes Service（Amazon EKS）失败情况：

- AWS FIS 实验或 Kubernetes 服务账号的 IAM 角色配置不正确。
  - 失败消息：
    - `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.`
  - 补救措施：验证以下内容。
    - 确保您已按照使用 AWS FISaws:eks:pod 操作中的说明进行操作。

    - 确保您已经创建并配置了具有必要的 RBAC 权限和正确命名空间的 Kubernetes 服务帐户。
    - 确保您已将提供的 IAM 角色（参见测试 AWS CloudFormation 堆栈的输出）映射到 Kubernetes 用户。
- 无法启动 AWS FIS Pod：已达到失败边车容器的最大值。当内存不足以运行 s AWS FIS idecar 容器时，通常会发生这种情况。
    - 失败消息：`Unable to heartbeat FIS Pod: Max failed sidecar containers reached`。
    - 补救措施：避免此错误的一种选择是降低目标负载百分比，使其与可用内存或 CPU 保持一致。
- 实验开始时警报断言失败。由于相关的警报没有数据点，因此出现此错误。
    - 失败消息：`Assertion failed for the following alarms`。列出断言失败的所有警报。
    - 补救措施：确保为警报正确安装了 Container Insights，并且警报未开启（处于 `ALARM` 状态）。

了解弹性分数

本节介绍如何 AWS Resilience Hub 量化不同中断情景下的应用程序就绪性。

AWS Resilience Hub 提供弹性分数，该分数代表应用程序的弹性状态。该分数反映了应用程序在满足应用程序弹性策略、警报、标准操作程序（SOP）和测试方面遵循我们的建议的程度。根据应用程序使用的资源类型，为每种中断类型 AWS Resilience Hub 推荐警报、SOP 和一组测试。

最高的弹性分数是 100 分。要获得尽可能高的分数或最高分，您必须在应用程序中实施所有推荐的警报、SOP 和测试。例如， AWS Resilience Hub 建议使用一个警报和一个 SOP 进行一次测试。测试运行并触发警报并启动相关的 SOP。如果它们成功运行，并且应用程序符合弹性策略，则其弹性分数将接近或等于 100 分。

运行首次评估后， AWS Resilience Hub 提供了从应用程序中排除操作建议的选项。要了解排除的建议对弹性分数的影响，您必须进行新的评测。但是，您可以随时在应用程序中包含排除的建议并进行新的评测。有关包括和排除警报、SOP 和测试建议的更多信息，请参阅 the section called “包含或排除操作建议”。

访问应用程序的“弹性分数”

您可以通过从导航菜单中选择控制面板或应用程序来查看应用程序的“弹性分数”。

从“控制面板”访问“弹性分数”

1. 在左侧导航窗格中，选择 VPC Dashboard。

2. 在随时间推移的应用程序弹性分数中，在最多选择 4 个应用程序下拉列表中选择一个或多个应用程序。
3. 弹性分数表显示所有选定应用程序的弹性分数。

从“应用程序”访问“弹性分数”

1. 在左侧的导航菜单中，选择应用程序。
2. 在应用程序中，打开一个应用程序。
3. 选择摘要。

   弹性分数表显示应用程序弹性分数最长一年的趋势。 AWS Resilience Hub 使用以下内容显示了为改善和实现尽可能高的弹性分数而需要解决的行动项目、弹性策略违规行为和操作建议：

   - 要查看为改善和实现尽可能高的弹性分数而需要完成的操作项，请选择操作项选项卡。选中后，AWS Resilience Hub 将显示以下内容：
     - RTO/RPO – 表示为解决应用程序弹性策略中的违例而需要修复的恢复时间（RTO/RPO）数量。选择该值以查看您的应用程序评测报告中的 RTO/RPO 详细信息。
     - 警报 — 表示需要在您的应用程序中实施的推荐的 Amazon CloudWatch 警报数量。选择该值以查看您的应用程序评估报告中需要修复的 Amazon CloudWatch 警报。
     - SOP – 表示需要在您的应用程序中实施的建议的 SOP 数量。选择该值以查看您的应用程序评测报告中需要修复的 SOP。
     - FIS – 表示需要在您的应用程序中实施的建议的测试数量。选择该值以查看您的应用程序评测报告中需要修复的测试。
   - 要查看影响您的弹性分数的每个组件的分数，请选择分数细分。选择后， AWS Resilience Hub 显示以下内容：
     - RTO/RPO 合规性 — 表示应用程序组件 (AppComponents) 与估计的工作负载恢复时间以及应用程序弹性策略中定义的目标恢复时间的兼容程度。选择该值以查看您的应用程序评测报告中的 RTO/RPO 估算值。
     - 已实施警报 — 表示已实施的 Amazon CloudWatch 警报的实际贡献与其对应用程序弹性分数的最大可能贡献的比较。选择该值，在您的应用程序的评估报告中查看已实施的 Amazon CloudWatch 警报。
     - 已实施的 SOP – 表示已实施的 SOP 的实际贡献与其对应用程序弹性分数的最大可能贡献的比较。选择该值以查看您的应用程序评测报告中的已实施 SOP。
     - 已实施的 FIS 实验 – 表示已实施的测试的实际贡献与其对应用程序弹性分数的最大可能贡献的比较。选择该值以查看您的应用程序评测报告中的已实施测试。

- 要查看弹性策略违例和操作建议，请选择向右箭头以展开策略违例和操作建议细分部分。展开后， AWS Resilience Hub 将显示以下内容：
  - 弹性策略违例 – 表示违反应用程序弹性策略的应用程序组件的数量。选择 RTO/RPO 旁边的值以查看您的应用程序评测报告中的弹性建议选项卡的详细信息。
  - 操作建议 – 表示为增强应用程序的弹性而尚未实施或执行的操作建议（使用未完成和已排除选项卡）。操作建议包括所有停用的建议和尚未执行的建议。

    要查看需要实施的操作建议，请选择未完成选项卡。选中后， AWS Resilience Hub 将显示以下内容：
    - 警报 — 表示需要实施的推荐的 Amazon CloudWatch 警报数量。
    - SOP – 表示需要实施的建议 SOP 的数量。
    - FIS – 表示需要实施的建议测试的数量。

    要查看应用程序中排除的操作建议，请选择已排除选项卡。选中后 AWS Resilience Hub 会显示以下内容：
    - 警报 — 表示从您的应用程序中排除的推荐的 Amazon CloudWatch 警报数量。
    - SOP – 表示从您的应用程序中排除的建议 SOP 的数量。
    - FIS – 表示从您的应用程序中排除的建议测试的数量。

计算弹性分数

本节中的表格说明了用于确定每种推荐类型的评分组成部分和应用程序的弹性分数的公式。 AWS Resilience Hub 由 AWS Resilience Hub 每种推荐类型的评分组成部分和应用程序的弹性分数确定的所有结果值都四舍五入到最接近的点。例如，如果实施了三分之二的警报，则分数将为 13.33（（2/3）* 20）分。该值将四舍五入为 13 点。有关表格中公式中使用的权重的更多信息，请参见 the section called “中断类型的权重 AppComponents 和中断类型” 部分。

有些评分组件只能通过 `ScoringComponentResiliencyScore` API 获得。相关此 API 的更多信息，请参阅 ScoringComponentResiliencyScore。

表

- 计算每种建议类型的评分组件的公式
- 计算弹性分数的公式
- 计算 AppComponents 和中断类型的弹性分数的公式

下表说明了用于计算每种推荐类型的评分部分的公式。 AWS Resilience Hub

计算每种建议类型的评分组件的公式

评分组件	描述	公式	示例
测试覆盖率（T）	标准化分数（0 -100 分）基于在 AWS Resilience Hub 建议测试总数中成功实施和排除的测试数量。 **Note** 要计算弹性分数，推荐的测试必须在过去 30 天内成功运行， AWS Resilience Hub 才能将其视为已实施。	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)` 部分公式如下： • 配置的测试总数-表示在 AWS CloudFormation 控制台中创建和上传 AWS CloudFormation 模板时配置的测试总数。 • 推荐的测试总数-表示 AWS Resilience Hub 根据应用程序资源推荐的测试。 • 排除的测试总数 - 表示您已从应用程序中排除的建议测试数量。	如果您实施了 AWS Resilience Hub 建议的 20 个测试中的 10 个测试并排除了 5 个测试，则测试覆盖率的计算方法如下： `T = (10 + 5) / 20` 即：`T = .75 or 75 points`
警报覆盖率（A）	标准化分数（0 -100 分），基于成功实施和排除的亚马逊 CloudWatch警报数量（在 AWS Resilience Hub 推荐的亚马逊 CloudWatch 警报总数中）。	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` 部分公式如下：	如果您在 AWS Resilience Hub 推荐的 20 个亚马逊 CloudWatch 警报中实施了 10 个但排除了 5 个亚马逊 CloudWatch 警报，则亚马逊 CloudWatch 警报覆

评分组件	描述	公式	示例
	Note 要计算弹性分数，建议的警报应处于就绪状态，以便 AWS Resilience Hub 将其视为已实施。	• 配置的警报总数-表示在 AWS CloudFormation 控制台中创建和上传 AWS CloudFormation 模板时配置的 Amazon CloudWatch 警报总数。 • 推荐的警报总数 — 表示 AWS Resilience Hub 根据应用程序资源推荐的 Amazon CloudWatch 警报。 • 排除的警报总数 — 表示您已从应用程序中排除的推荐的 Amazon CloudWatch 警报数量。	盖范围的计算方法如下： `A = (10 + 5) / 20` 即：`A = .75 or 75 points`

评分组件	描述	公式	示例
SOP 覆盖率（S）	标准化分数（0 - 100 分）基于成功实施并排除的 SOP 数量在 AWS Resilience Hub 建议的 SOP 警报总数中的数量。	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` 部分公式如下： • 配置的 SOP 总数-表示在控制台中创建和上传 AWS CloudFormation 模板时配置的 SOP 总数。AWS CloudFormation • 推荐的 SOP 总数-表示 AWS Resilience Hub 根据应用程序资源推荐的 SOP。 • 排除的 SOP 总数 - 表示您已从应用程序中排除的建议 SOP 的数量。	如果您实施了 AWS Resilience Hub 建议的 20 个 SOP 中的 10 个 SOP 并排除了 5 个 SOP，则 SOP 覆盖率的计算方法如下： `S = (10 + 5) / 20` 即：`S = .75 or 75 points`

评分组件	描述	公式	示例

RTO/RPO 合规性（P）	基于符合其弹性策略的应用程序的标准化分数（0 - 100 分）。	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	如果您的应用程序弹性策略仅适用于可用区（AZ）和基础设施中断类型，则弹性策略分数（P）的计算方法如下：
			• 如果您设定了区域 RTO 和 RPO 目标，则 P 的计算方法如下：
			`P = (20 + 30)/ 100`
			即：`P = .5 or 50 points`
			• 如果您尚未设定区域 RTO 和 RPO 目标，则 P 的计算方法如下：
			`P = (22.22 + 33.33)/ 99.9`
			即：`P = .55 or 55 points`

下表说明了用于计算整个应用程序的弹性分数的公式。 AWS Resilience Hub

计算弹性分数的公式

评分组件	描述	公式	示例
应用程序的弹性分数（RS）	基于您的应用程序满足其弹性策略的标准化弹性分数（0 - 100 分）。每个应用程序的弹性分数是所有建议类型的加权平均值。即：RS = Weighted Average (T, A, S, P)	使用以下公式计算每个应用程序的弹性分数：RS = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	计算每种建议类型表的覆盖率的公式如下： • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 每个应用程序的弹性分数计算方法如下： RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4) 即：RS = .65 or 65 points

下表说明了用于计算应用程序组件 (AppComponents) 和中断类型的弹性分数的公式。 AWS Resilience Hub 但是，您只能通过以下 AWS Resilience Hub API 获取弹性分数 AppComponents 和中断类型：

- DescribeAppAssessment以获得 RSo
- ListAppComponentCompliances获取RSao和 RSA

计算 AppComponents 和中断类型的弹性分数的公式

评分组件	描述	公式	示例
每种中断类型 AppComponent 和每种中断类型的弹性得分 () RSao	基于 AppComponent 满足每种中断类型的弹性策略的标准化分数（0-100 分）。每种中断类型 AppComponent 和每种中断类型的弹性分数是所有建议类型的加权平均值。 即：RSao = Weighted Average (T, A, S, P) 的值T, A, S, P是针对和中断类型的所有推荐测试、警报、SOP 和会议弹性策略计算得出的。	使用以下公式计算每种中断类型 AppComponent 和每种中断类型的弹性分数： RSao = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	所有建议类型的 RSao 假设如下： • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 每 AppComponent 种中断类型的弹性分数的计算方法如下： RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) 即：RSao = .65 or 65 points

评分组件	描述	公式	示例
	AppComponent		
每 AppComponent () RSa 的弹性分数	基于满足其弹性策略的标准化分数（0 - 100 分）。弹性分数 AppComponent 是所有建议类型的加权平均值。即：RSa = Weighted Average (T, A, S, P) 的值T, A, S, P是针对的所有推荐测试、警报、SOP 和会议弹性策略计算得出的。AppComponent	每人的弹性分数 AppComponent 是使用以下公式计算的： RSa = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	所有建议类型的 RSa 假设如下： • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 每个弹性分数的计算方法 AppComponent 如下： RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) 即：RSa = .65 or 65 points

评分组件	描述	公式	示例
每种中断类型的弹性分数（RSo）	基于满足其弹性策略的标准化分数（0 - 100 分）。每种中断类型的弹性分数是所有建议类型的加权平均值。即：RSo = Weighted Average (T, A, S, P) T, A, S, P 的值针对中断类型的所有建议测试、警报、SOP 和会议弹性策略计算得出。	每种中断类型的弹性分数使用以下公式计算： RSo = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	所有建议类型的 RSo 假设如下： • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 每种中断类型的弹性分数的计算方法如下： RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) / (.2 + .2 + .2 + .4) 即：RSo = .65 or 65 points

Weight

AWS Resilience Hub 为每种建议类型分配总弹性分数的权重。

下表显示了警报、SOP、测试、会议弹性策略和中断类型的权重。中断类型包括应用程序、基础设施、可用区和区域。

> **Note**
>
> 如果您选择不为策略定义区域 RTO 或 RPO 目标，则其他中断类型的权重会相应增加，如未定义区域时的权重列所示。

警报、SOP、测试、策略目标的权重

获取建议	权重
告警	20 点数
SOP	20 点数
测试	20 点数
会议弹性策略	40 点数

中断类型的权重

中断类型	定义区域时的权重	未定义区域时的权重
应用程序	40 点数	44.44 点数
基础设施	30 点数	33.33 点数
可用区	20 点数	22.22 点数
区域	10 点数	不适用

通过 AWS CloudFormation 将操作建议集成到您的应用程序中

在操作建议页面中选择创建 CloudFormation 模板后，AWS Resilience Hub 创建一个描述应用程序的特定警报、标准操作程序 (SOP) 或 AWS FIS 实验的 AWS CloudFormation 模板。AWS CloudFormation 模板存储在 Amazon S3 存储桶中，您可以在操作建议页面的模板详细信息选项卡中查看模板的 S3 路径。

例如，下面的列表显示了一个 JSON 格式的 AWS CloudFormation 模板，该模板描述了由 AWS Resilience Hub 提供的警报建议。这是名为 `Employees` 的 DynamoDB 表的读取限制警报。

模板的 Resources 部分描述了 DynamoDB 表的读取限制事件数量超过 1 时激活的 AWS::CloudWatch::Alarm 警报。这两个 AWS::SSM::Parameter 资源定义了元数据，这些元数据允许 AWS Resilience Hub 在不扫描实际应用程序的情况下识别已安装的资源。

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the 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."
      }
    }
  }
```

```
}
```

修改 AWS CloudFormation 模板。

要将警报、SOP 或 AWS FIS 资源集成到您的主应用程序中，最简单的方法就是将其作为另一个资源添加到描述您的应用程序模板的模板中。下面提供的 JSON 格式文件提供了 AWS CloudFormation 模板中如何描述 DynamoDB 表的基本概述。一个真实的应用程序可能还会包含更多资源，例如额外的表。

```
{
   "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"
                  }
               }
            ]
         }
      }
   }
```

```
}
```

要允许在应用程序中部署警报资源，您现在需要将硬编码资源替换为应用程序堆栈中的动态引用。

因此，在 AWS::CloudWatch::Alarm 资源定义中，将以下内容：

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

更改为：

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

在 AWS::SSM::Parameter 资源定义下，将以下内容：

```
"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\"]}"
```

更改为：

```
"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\"]}"
```

在修改 SOP 和 AWS FIS 实验的 AWS CloudFormation 模板时，您将采用相同的方法，将硬编码的引用 ID 替换为即使在硬件更改后仍能继续工作的动态引用。

通过使用对 DynamoDB 表的引用，您允许 AWS CloudFormation 执行以下操作：

- 首先创建数据库表。
- 始终在警报中使用生成的资源的实际 ID，如果 AWS CloudFormation 需要替换资源，则动态更新警报。

> **Note**
>
> 您可以使用 AWS CloudFormation 选择更高级的方法来管理应用程序资源，例如嵌套堆栈或在单独的 AWS CloudFormation 堆栈中引用资源输出。（但是，如果要将建议堆栈与主堆栈分开，则需要配置一种在两个堆栈之间传递信息的方式。）
> 此外，第三方工具，例如 HashiCorp 的 Terraform，也可以用来配置基础设施即代码 (IaC)。

使用 AWS Resilience Hub API 描述和管理应用程序

作为使用 AWS Resilience Hub 控制台描述和管理应用程序的替代方案，AWS Resilience Hub 允许您使用 AWS Resilience Hub API 描述和管理应用程序。本章节介绍如何使用 AWS Resilience Hub API 创建应用程序。另外，还定义了执行 API 所需的顺序，以及您必须提供带有相应示例的参数值。有关更多信息，请参阅以下主题：

- the section called “准备应用程序”
- the section called “运行和分析应用程序”
- the section called “修改您的应用程序”

步骤 1：准备应用程序

要准备应用程序，必须先创建应用程序，分配弹性策略，然后从输入源导入应用程序资源。有关准备应用程序所用的 AWS Resilience Hub API 的更多信息，请参阅以下主题：

- the section called “创建应用程序”
- the section called “创建弹性策略”
- the section called “导入应用程序资源并监控导入状态”
- the section called “发布您的应用程序并分配弹性策略”

创建应用程序

要在 AWS Resilience Hub 中创建新应用程序，必须调用 `CreateApp` API 并提供唯一的应用程序名称。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html。

以下示例演示了如何在 AWS Resilience Hub 中使用 `CreateApp` API 创建新应用程序 `newApp`。

请求

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

响应

```
{
```

```
    "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"
    }
}
```

创建弹性策略

创建应用程序后，必须创建弹性策略，以便能够使用 `CreateResiliencyPolicy` API 了解应用程序的弹性状态。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html。

以下示例演示了如何在 AWS Resilience Hub 中使用 `CreateResiliencyPolicy` API 为您的应用程序创建 `newPolicy`。

请求

```
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}}'
```

响应

```
{
    "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": {}
    }
}
```

从输入源导入资源并监控导入状态

AWS Resilience Hub 提供了以下 API 以将资源导入您的应用程序：

- `ImportResourcesToDraftAppVersion` — 此 API 允许您将来自不同输入源的资源导入应用程序的草稿版本。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html。
- `PublishAppVersion` — 此 API 发布应用程序的新版本以及更新后的 AppComponents。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html。
- `DescribeDraftAppVersionResourcesImportStatus` — 此 API 允许您监控向某个应用程序版本导入资源时的导入状态。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html。

以下示例演示了如何在 AWS Resilience Hub 中使用 `ImportResourcesToDraftAppVersion` API 将资源导入应用程序。

请求

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

响应

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

以下示例演示了如何在 AWS Resilience Hub 中使用 `CreateAppVersionResource` API 手动向应用程序添加资源。

请求

```
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"]'
```

响应

```
{
    "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"
            }
        ]
    }
}
```

以下示例演示了如何在 AWS Resilience Hub 中使用 `DescribeDraftAppVersionResourcesImportStatus` API 监控资源的导入状态。

请求

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

响应

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

发布您的应用程序的草稿版本并分配弹性策略

在运行评估之前，必须先发布应用程序的草稿版本，并为已发布的应用程序版本分配弹性策略。

发布您的应用程序的草稿版本并分配弹性策略

1. 要发布应用程序的草稿版本，请使用 `PublishAppVersion` API。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html。

   以下示例演示了如何在 AWS Resilience Hub 中使用 `PublishAppVersion` API 发布应用程序的草稿版本。

请求

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

响应

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

2. 使用 UpdateApp API 将弹性策略应用于已发布的应用程序版本。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html。

以下示例演示了如何在 AWS Resilience Hub 中使用 UpdateApp API 将弹性策略应用于已发布的应用程序版本。

请求

```
aws resiliencehub update-app \
--app-arn <App_ARN> \
--policy-arn <Policy_ARN>
```

响应

```
{
    "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"
    }
}
```

步骤 2：运行和管理 AWS Resilience Hub 弹性评估

发布应用程序的新版本后，必须运行新的弹性评估并分析结果，以确保您的应用程序满足弹性策略中定义的估计的工作负载 RTO 和估计的 RPO。评估会将每个应用程序组件配置与策略进行比较，并提出警报、SOP 和测试建议。

有关更多信息，请参阅以下主题：

- the section called “运行和监控弹性评估”
- the section called “创建弹性策略”

运行和监控 AWS Resilience Hub 弹性评估

要在 AWS Resilience Hub 中运行弹性评估并监控其状态，必须使用以下 API：

- `StartAppAssessment` — 此 API 为应用程序创建新的评估。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html。
- `DescribeAppAssessment` — 此 API 描述应用程序的评估并提供评估的完成状态。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html。

以下示例演示了如何在 AWS Resilience Hub 中使用 `StartAppAssessment` API 开始运行新的评估。

请求

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

响应

```
{
    "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": {}
    }
}
```

以下示例演示了如何在 AWS Resilience Hub 中使用 `DescribeAppAssessment` API 监控评估状态。您可以从 `assessmentStatus` 变量中提取评估状态。

请求

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

响应


```
{
    "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": {}
    }
}
```

检查评估结果

成功完成评估后，您可以使用以下 API 检查评估结果。

- `DescribeAppAssessment` — 此 API 允许您根据弹性策略跟踪应用程序的当前状态。此外，您还可以从 `complianceStatus` 变量中提取合规性状态，并从 `resiliencyScore` 结构中提取每种中断类型的弹性得分。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html。
- `ListAlarmRecommendations` — 此 API 允许您使用评估的 Amazon 资源名称 (ARN) 来获取警报建议。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html。

> **Note**
>
> 要获取 SOP 和 FIS 测试建议，请使用 ListSopRecommendations 和 ListTestRecommendations API。

以下示例演示了如何在使用 ListAlarmRecommendations API 的情况下使用评估的 Amazon 资源名称 (ARN) 获取警报建议。

> **Note**
>
> 要获取 SOP 和 FIS 测试建议，请改为使用 ListSopRecommendations 或 ListTestRecommendations。

请求

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

响应

```
{
    "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 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": "Alarm by AWS ResilienceHub that reports when 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": "Alarm by AWS ResilienceHub 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": "Alarm by AWS ResilienceHub 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": "Alarm by AWS ResilienceHub 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": "Alarm by AWS ResilienceHub 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": "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>)."
        }
    ]
}
```

以下示例演示了如何使用 ListAppComponentRecommendations API 获取配置建议（有关如何提高当前弹性的建议）。

请求

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

响应

```
{
    "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
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
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 ECS service with launch type EC2 and EFS
storage, deployed in multiple AZs. AWS Backup is used to backup EFS and copy snapshots
in-region.",
                    "suggestedChanges": [
                        "Add Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove 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 EFS from backup.
(Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for EFS
from backups, derived from backup frequency"
                        }
```

```
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "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 EFS from backup.
(Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for EFS
from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAttainable",
                    "description": "EFS with backups configured",
                    "suggestedChanges": [
```

```
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                }
            ]
        }
    ]
}
```

步骤 3：修改您的应用程序

AWS Resilience Hub 允许您通过编辑应用程序的草稿版本并将更改发布到新（已发布）版本来修改应用程序资源。AWS Resilience Hub 使用应用程序的已发布版本（包括更新后的资源）来运行弹性评估。

有关更多信息，请参阅以下主题：

- the section called “手动添加资源”
- the section called “将资源分组到单个应用程序组件”
- the section called “从 AppComponent 中排除资源”

手动向应用程序添加资源

如果资源不是作为输入源的一部分而部署，则 AWS Resilience Hub 允许您使用 `CreateAppVersionResource` API 手动向应用程序添加资源。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html。

您必须向此 API 提供以下参数：

- 应用程序的 Amazon 资源名称 (ARN)
- 资源的逻辑 ID
- 资源的物理 ID
- AWS CloudFormation 类型

以下示例演示了如何在 AWS Resilience Hub 中使用 `CreateAppVersionResource` API 手动向应用程序添加资源。

请求

```
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"]'
```

响应

```
{
    "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"
            }
        ]
    }
}
```

将资源分组到单个应用程序组件

应用程序组件 (AppComponent) 是一组相关的 AWS 资源，它们作为一个单元起作用和失效。例如，当您的跨区域工作负载用作备用部署时。AWS Resilience Hub 具有管理哪些 AWS 资源可以属于哪种类型的 AppComponent 的规则。AWS Resilience Hub 允许您使用以下资源管理 API 将资源分组到单个 AppComponent 中。

- `UpdateAppVersionResource` — 此 API 更新应用程序的资源详细信息。有关此 API 的更多信息，请参阅 UpdateAppVersionResource。
- `DeleteAppVersionAppComponent` — 此 API 从应用程序中删除 AppComponent。有关此 API 的更多信息，请参阅 DeleteAppVersionAppComponent。

以下示例演示了如何在 AWS Resilience Hub 中使用 `DeleteAppVersionAppComponent` API 更新应用程序的资源详细信息。

请求

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

响应

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

以下示例演示了如何在 AWS Resilience Hub 中使用 `UpdateAppVersionResource` API 删除前面示例中创建的空 AppComponent。

请求

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

响应

```
{
    "appArn": "<App_ARN>",
```

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

从 AppComponent 中排除资源

AWS Resilience Hub 许您使用 UpdateAppVersionResource API 从评估中排除资源。在计算应用程序弹性时，不会考虑这些资源。相关此 API 的更多信息，请参阅 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html。

> **Note**
>
> 您只能排除从输入源导入的那些资源。

以下示例演示了如何在 AWS Resilience Hub 中使用 UpdateAppVersionResource API 排除应用程序资源。

请求

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

响应

```
{
    "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"
            }
        ]
    }
}
```

安全性 AWS Resilience Hub

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 AWS Resilience Hub，请参阅按合规计划划分的范围内的 AWSAWS 服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用时如何应用分担责任模型 AWS Resilience Hub。以下主题向您介绍如何进行配置 AWS Resilience Hub 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AWS Resilience Hub 资源。

内容

中的数据保护 AWS Resilience Hub

分 AWS 担责任模型适用于中的数据保护 AWS Resilience Hub。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用 multi-factor authentication（ MFA ）。

- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括 AWS 服务 使用控制台、API 或 AWS SDK 与 Resilitions Hub 或其他平台合作时。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

AWS Resilience Hub 对您的静态数据进行加密。中的数据使用透明 AWS Resilience Hub 的服务器端加密进行静态加密。这样可以帮助减少在保护敏感数据时涉及的操作负担和复杂性。通过静态加密，您可以构建符合加密合规性和法规要求的安全敏感型应用程序。

传输中加密

AWS Resilience Hub 对服务与其他集成 AWS 服务之间传输的数据进行加密。在 AWS Resilience Hub 和集成服务之间传递的所有数据均使用传输层安全 (TLS) 进行加密。 AWS Resilience Hub 为跨 AWS 服务的特定类型的目标提供预配置的操作，并支持针对目标资源的操作。

AWS 弹性中心的 Identity and Access 管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）使用 AWS 弹性中心资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 使用策略管理访问
- AWS 弹性中心如何与 IAM 配合使用
- IAM 角色和权限
- 故障排除 AWS 弹性中心身份和访问权限
- AWS Resilience Hub 访问权限参考
- AWS 的托管策略 AWS Resilience Hub
- 将 Terraform 状态文件导入 AWS Resilience Hub
- 允许 AWS Resilience Hub 访问您的亚马逊 Elastic Kubernetes Service 集群
- 允许发布 AWS Resilience Hub 到您的 Amazon 简单通知服务主题
- 限制包含或排除 AWS Resilience Hub 推荐的权限

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Resilience Hub AWS 中所做的工作。

服务用户-如果您使用 Res AWS ilience Hub 服务完成工作，则您的管理员会为您提供所需的凭据和权限。当你使用更多 Res AWS ilience Hub 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Resilience Hub AWS 中的某项功能，请参阅故障排除 AWS 弹性中心身份和访问权限。

服务管理员 — 如果你负责公司的 Resilience Hub 资源，那么你可能拥有对 Resilience Hub 的 AWS 完全访问权限。 AWS 您的工作是确定您的服务用户应访问哪 AWS 些 Resilience Hub 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解您的公司如何将 IAM 与 Resilience Hu AWS b 配合使用，请参阅AWS 弹性中心如何与 IAM 配合使用。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理对 Resilience Hub AWS 的访问权限。要查看您可以在 IAM 中使用的基于身份的 Resilience Hub 策略示例 AWS ，请参阅。Resilience Hub 基于身份的 AWS 策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS ）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （ IAM Identity Center ）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证 和《IAM 用户指南》中的 在 AWS中使用多重身份验证（ MFA ）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。

- 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
- 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其它策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 - 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管

理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。

- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

AWS 弹性中心如何与 IAM 配合使用

在使用 IAM 管理对 AWS 弹性中心的访问权限之前，请先了解哪些可用于 Resilience Hub 的 IAM 功能。 AWS

您可以与 AWS 弹性中心一起使用的 IAM 功能

IAM 功能	AWS 弹性中心支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	支持
策略条件键（特定于服务）	支持
ACL	否
ABAC（策略中的标签）	部分
临时凭证	支持
转发访问会话（FAS）	支持

IAM 功能	AWS 弹性中心支持
服务角色	支持

要全面了解 Resilience Hub 和其他 AWS 服务如何 AWS 与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

弹性中心的基于身份的 AWS 策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Resilience Hub 基于身份的 AWS 策略示例

要查看 Resilienc AWS e Hub 基于身份的策略示例，请参阅。Resilience Hub 基于身份的 AWS 策略示例

AWS 弹性中心内基于资源的策略

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时

AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

AWS 弹性中心的政策行动

支持策略操作	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Resilienc AWS e Hub 操作列表，请参阅《服务授权参考》中的 AWS Resilience Hub 定义的操作。

Resilien AWS ce Hub 中的策略操作在操作前使用以下前缀：

```
resiliencehub
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 Resilienc AWS e Hub 基于身份的策略示例，请参阅。Resilience Hub 基于身份的 AWS 策略示例

AWS 弹性中心的政策资源

支持策略资源	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 AWS 弹性中心资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 Res ili AWS ence Hub 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 Resilience H ub 定义的操作 AWS 。

要查看 Resilienc AWS e Hub 基于身份的策略示例，请参阅。Resilience Hub 基于身份的 AWS 策略示例

AWS 弹性中心的策略条件密钥

支持特定于服务的策略条件键	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Resilienc AWS e Hub 条件密钥列表，请参阅《服务授权参考》中的 AWS Resilience Hub 条件密钥。要了解您可以使用哪些操作和资源使用条件键，请参阅 Resilience Hub AWS 定义的操作。

要查看 Resilienc AWS e Hub 基于身份的策略示例，请参阅。Resilience Hub 基于身份的 AWS 策略示例

AWS 弹性中心中的 ACL

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

带有 AWS 弹性中心的 ABAC

支持 ABAC（策略中的标签）	部分

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在 AWS 弹性中心使用临时证书

支持临时凭证	支持

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IAM 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

AWS 弹性中心的转发访问会话

支持转发访问会话 (FAS)	支持

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

AWS 弹性中心的服务角色

支持服务角色	支持

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 Resilience AWS Hub 的功能。仅当 Resilience AWS Hub 提供相关指导时才编辑服务角色。

Resilience Hub 基于身份的 AWS 策略示例

默认情况下，用户和角色无权创建或修改 Resilience AWS Hub 资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM policy。

有关 Resilience Hub 定义的操作和资源类型（包括每种资源类型的 ARN 格式）的详细信息，请参阅《服务授权参考》中的 Resilience Hub 的操作、资源和条件密钥。 AWS AWS

主题

- 策略最佳实践
- 使用 AWS 弹性中心控制台
- 允许用户查看他们自己的权限
- 列出可用的 AWS Resilience Hub 应用程序
- 开始应用程序评估
- 删除应用程序评估
- 为特定应用程序创建推荐模板
- 删除特定应用程序的推荐模板
- 使用特定的弹性策略更新应用程序

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 Resili AWS ence Hub 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对

您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的AWS 托管策略。

- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 AWS 弹性中心控制台

要访问 Resil AWS ience Hub 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Resilien AWS ce Hub 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Resilience Hub 控制台，还需要将 AWS 弹性中心*ConsoleAccess*或*ReadOnly* AWS 托管策略附加到实体。 AWS 有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

以下策略授予用户在 AWS Resilience Hub 控制台中列出和查看所有资源的权限，但不允许创建、更新或删除这些资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "resiliencehub:List*",
                "resiliencehub:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

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

列出可用的 AWS Resilience Hub 应用程序

以下策略授予用户列出可用 AWS Resilience Hub 应用程序的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

开始应用程序评估

以下政策授予用户开始对特定 AWS Resilience Hub 应用程序进行评估的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
```

```
  ]
}
```

删除应用程序评估

以下策略授予用户删除特定 AWS Resilience Hub 应用程序评估的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

为特定应用程序创建推荐模板

以下策略授予用户为特定 AWS Resilience Hub 应用程序创建推荐模板的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

删除特定应用程序的推荐模板

以下策略授予用户删除特定 AWS Resilience Hub 应用程序的推荐模板的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

使用特定的弹性策略更新应用程序

以下策略授予用户使用特定弹性策略更新 AWS Resilience Hub 应用程序的权限。

```
{
  "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/*" }
      }
    }
  ]
}
```

IAM 角色和权限

AWS Resilience Hub 允许您在为应用程序运行评估时配置要使用的 IAM 角色。您可以通过多种方式配置 AWS Resilience Hub ，以获得对应用程序资源的只读访问权限。但是， AWS Resilience Hub 建议使用以下方法：

- 基于角色的访问权限-此角色是在当前账户中定义和使用的。 AWS Resilience Hub 将担任此角色来访问您的应用程序的资源。

  要提供基于角色的访问权限，该角色必须包括以下内容：

  - 读取资源的只读权限（ AWS Resilience Hub 建议您使用`AwsResilienceHubAssessmentPolicy`托管策略）。
  - 担任此角色的信任策略，允许 AWS Resilience Hub 服务负责人担任此角色。如果您的账户中没有配置此类角色， AWS Resilience Hub 将显示创建该角色的说明。有关更多信息，请参阅 the section called “步骤 6：设置权限”。

  > **Note**
  >
  > 如果您仅提供调用者角色名称，并且您的资源位于其他账户中，则 AWS Resilience Hub 将在其他账户中使用此角色名称来访问跨账户资源。或者，您可以为其他账户配置角色 ARN，该角色 ARN 将用于代替调用者角色名称。

- 当前 IAM 用户访问权限 – AWS Resilience Hub 将使用当前 IAM 用户访问您的应用程序资源。当您的资源位于不同的账户中时， AWS Resilience Hub 将扮演以下 IAM 角色来访问这些资源：
  - `AwsResilienceHubAdminAccountRole`，在当前账户中
  - `AwsResilienceHubExecutorAccountRole`，在其他账户中

  此外，在配置定期评估时， AWS Resilience Hub 将担任该`AwsResilienceHubPeriodicAssessmentRole`角色。但是，不建议使用`AwsResilienceHubPeriodicAssessmentRole`，因为您必须手动配置角色和权限，而且某些功能（例如弹性偏差检测）可能无法按预期运行。

故障排除 AWS 弹性中心身份和访问权限

使用以下信息来帮助您诊断和修复在使用 Resilience Hub 和 IAM 时可能遇到的常见问题。 AWS

主题

- 我无权在 Resilience Hub AWS 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人访问我的 Resil AWS 账户 ience AWS Hub 资源

我无权在 Resilience Hub AWS 中执行操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 resiliencehub:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 resiliencehub:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 resiliencehub:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一条错误消息，指出您无权执行该iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 Resilience H AWS ub。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在 Resilience Hub 中 AWS 执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我的 Resil AWS 账户 ience AWS Hub 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Resili AWS ence Hub 是否支持这些功能，请参阅AWS 弹性中心如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户存取之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

AWS Resilience Hub 访问权限参考

您可以使用 AWS Identity and Access Management (IAM) 来管理对应用程序资源的访问权限，并创建适用于用户、群组或角色的 IAM 策略。

可以将每个 AWS Resilience Hub 应用程序配置为使用the section called “调用者角色”（一个 IAM 角色）或使用当前 IAM 用户权限（以及一组用于跨账户和定期评估的预定义角色）。在此角色中，您可以附加一个策略，该策略定义了 AWS Resilience Hub 访问其他 AWS 资源或应用程序资源所需的权限。调用者角色必须具有添加到 AWS Resilience Hub 服务主体的信任策略。

要管理应用程序的权限，我们建议使用 the section called “AWS 托管策略”。您可以使用这些托管式策略，而无需做任何修改，也可以将它们作为起点编写自己的限制性策略。策略可以通过操作影响的资源以及其他可选条件来限制用户权限。

如果您的应用程序资源位于不同的账户（辅助账户/资源账户）中，则必须在包含您的应用程序资源的每个账户中设置一个新角色。

主题

- the section called “使用 IAM 角色”

- the section called “使用当前的 IAM 用户权限”

使用 IAM 角色

AWS Resilience Hub 将使用预定义的现有 IAM 角色访问您在主账户或辅助账户/资源账户中的资源。这是访问您的资源的推荐权限选项。

主题

- the section called “调用者角色”
- the section called “不同 AWS 账户中的角色用于跨账户访问”

调用者角色

AWS Resilience Hub 调用者角色是一个 AWS Identity and Access Management (IAM) 角色， AWS Resilience Hub 用于访问 AWS 服务和资源。例如，您可以创建一个有权限访问您的 CFN 模板及其创建的资源的调用者角色。此页面提供有关如何创建、查看和管理应用程序调用者角色的信息。

创建应用程序时，您需要提供调用者角色。当您导入资源或开始评测时， AWS Resilience Hub 担任这个角色来访问您的资源。 AWS Resilience Hub 为了正确扮演您的调用者角色，角色的信任策略必须将 AWS Resilience Hub 服务主体 (r esiliencehub.amazonaws.com) 指定为可信服务。

要查看应用程序的调用者角色，请从导航窗格中选择应用程序，然后从应用程序页面的操作菜单中选择更新权限。

可以随时在应用程序调用者角色中添加或删除权限，或配置您的应用程序以使用不同的角色访问应用程序资源。

主题

- the section called “在 IAM 控制台中创建一个角色”
- the section called “使用 IAM API 管理角色”
- the section called “使用 JSON 文件定义信任策略”

在 IAM 控制台中创建一个角色

AWS Resilience Hub 要允许访问 AWS 服务和资源，您必须使用 IAM 控制台在主账户中创建调用者角色。有关使用 IAM 控制台创建角色的更多信息，请参阅为 AWS 服务创建角色（控制台）。

要使用 IAM 控制台在主账户中创建调用者角色

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 从导航窗格中选择角色，然后选择创建角色。
3. 选择自定义信任策略，在自定义信任策略窗口中复制以下策略，然后选择下一步。

> **Note**
>
> 如果您的资源位于不同的账户中，则必须在每个账户中创建一个角色，并对其他账户使用辅助账户信任策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 在添加权限页面的权限策略部分，在按属性或策略名称筛选策略然后按 Enter 框中输入 AWSResilienceHubAsssessmentExecutionPolicy。
5. 选择策略，然后选择下一步。
6. 在角色详细信息部分，在角色名称框中输入唯一的角色名称（例如 AWSResilienceHubAssessmentRole）。

   此字段仅接受字母数字和“+=,.@-_/”字符。
7. （可选）在描述框中，为存储库输入描述。
8. 请选择 创建角色。

   要编辑角色的使用案例和权限，在 步骤 1：选择可信实体 或 步骤 2：添加权限部分中选择 编辑。

创建调用者角色和资源角色后（如果适用），您可以配置应用程序以使用这些角色。

> **Note**
>
> 创建或更新应用程序时，您的当前 IAM 用户/角色必须拥有对调用者角色的 `iam:passRole` 权限。但是，您不需要此权限即可运行评测。

使用 IAM API 管理角色

角色的信任策略会向指定主体授予代入该角色的权限。要使用 AWS Command Line Interface (AWS CLI) 创建角色，请使用`create-role`命令。在使用此命令时，您可以指定内联信任策略。以下示例说明如何向 AWS Resilience Hub 服务授予担任您角色的委托人权限。

> **Note**
>
> JSON 字符串中对转义引号（ ' ' ）的要求可能因 shell 版本而异。

示例 **`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"
    }
  ]
}'
```

使用 JSON 文件定义信任策略

您还可以使用单独的 JSON 文件为角色定义信任策略，然后运行 `create-role` 命令。在下面的示例中，**`trust-policy.json`** 是位于当前目录中的一个文件。通过运行 **`create-role`** 命令将此策略附加到角色。**`create-role`** 命令的输出显示在示例输出中。要为角色添加权限，请使用attach-policy-to-role命令，然后您可以先添加`AWSResilienceHubAsssessmentExecutionPolicy`托管策略。有关托管策略的更多信息，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

示例 **`trust-policy.json`**

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "resiliencehub.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }]
}
```

示例 **create-role**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-document file://trust-policy.json
```

示例输出

```
{
    "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"
            }]
        }
    }
}
```

示例 **attach-policy-to-role**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

用于跨账户访问的不同 AWS 账户中的角色——可选

当您的资源位于辅助/资源账户中时，您必须在每个账户中创建角色 AWS Resilience Hub 才能成功评估您的应用程序。角色创建过程与调用者角色创建过程类似，但信任策略配置除外。

> **Note**
>
> 您必须在资源所在的辅助账户中创建角色。

主题

- the section called “在 IAM 控制台中为辅助账户/资源账户创建角色”
- the section called “使用 IAM API 管理角色”
- the section called “使用 JSON 文件定义信任策略”

在 IAM 控制台中为辅助账户/资源账户创建角色

AWS Resilience Hub 要允许访问其他 AWS 账户中的 AWS 服务和资源，您必须在每个账户中创建角色。

使用 IAM 控制台在 IAM 控制台中为辅助账户/资源账户创建角色

1. 使用 `https://console.aws.amazon.com/iam/` 打开 IAM 控制台。
2. 从导航窗格中选择角色，然后选择创建角色。
3. 选择自定义信任策略，在自定义信任策略窗口中复制以下策略，然后选择下一步。

> **Note**
>
> 如果您的资源位于不同的账户中，则您必须在每个账户中创建一个角色，并对其他账户使用辅助账户信任策略。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 在添加权限页面的权限策略部分，在按属性或策略名称筛选策略然后按 Enter 框中输入 AWSResilienceHubAsssessmentExecutionPolicy。
5. 选择策略，然后选择下一步。
6. 在角色详细信息部分，在角色名称框中输入唯一的角色名称（例如 AWSResilienceHubAssessmentRole）。
7. （可选）在描述框中，为存储库输入描述。
8. 请选择 创建角色。

   要编辑角色的使用案例和权限，在 步骤 1：选择可信实体 或 步骤 2：添加权限 部分中选择 编辑。

此外，您还需要向调用者角色添加 sts:assumeRole 权限，使其能够担任您的辅助账户中的角色。

将以下策略添加到您创建的每个辅助角色的调用者角色中：

```
{
    "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"
      ]
}
```

使用 IAM API 管理角色

角色的信任策略会向指定主体授予代入该角色的权限。要使用 AWS Command Line Interface (AWS CLI) 创建角色，请使用`create-role`命令。在使用此命令时，您可以指定内联信任策略。以下示例说明如何向 AWS Resilience Hub 服务主体授予代入您的角色的权限。

> **Note**
>
> JSON 字符串中对转义引号（`\'`）的要求可能因 shell 版本而异。

示例 **`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"}]}'
```

您还可以使用单独的 JSON 文件为角色定义信任策略。在下面的示例中，`trust-policy.json` 是位于当前目录中的一个文件。

使用 JSON 文件定义信任策略

您还可以使用单独的 JSON 文件为角色定义信任策略，然后运行 `create-role` 命令。在下面的示例中，**`trust-policy.json`** 是位于当前目录中的一个文件。通过运行 **`create-role`** 命令将此策略附加到角色。**`create-role`** 命令的输出显示在示例输出中。要为角色添加权限，请使用attach-policy-to-role命令，您可以先添加AWSResilienceHubAsssessmentExecutionPolicy托管策略。有关托管策略的更多信息，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

示例 **`trust-policy.json`**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

示例 **create-role**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document file://trust-policy.json
```

示例输出

```
{
    "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"
                }
            ]
        }
    }
}
```

示例 **attach-policy-to-role**

aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --policy-arn arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy.

使用当前的 IAM 用户权限

如果您想使用当前的 IAM 用户权限来创建和运行评测，请使用此方法。您可以将 AWSResilienceHubAsssessmentExecutionPolicy 托管式策略附加到您的 IAM 用户或与用户关联的角色。

单个账户设置

使用上述托管式策略足以对与 IAM 用户使用同一账户托管的应用程序进行评测。

计划评测设置

您必须创建一个新角色 AwsResilienceHubPeriodicAssessmentRole 以使 AWS Resilience Hub 执行与计划评测相关的任务。

> **Note**
>
> - 使用基于角色的访问权限（使用上面提到的调用者角色）时，不需要执行此步骤。
> - 角色名称必须为 AwsResilienceHubPeriodicAssessmentRole。

AWS Resilience Hub 要允许执行与计划评估相关的任务

1. 将 AWSResilienceHubAsssessmentExecutionPolicy 托管式策略附加到角色。
2. 添加以下策略，其中primary_account_id是定义应用程序并将运行评估的 AWS 账户。此外，您必须为定期评估的角色添加关联的信任策略 (AwsResilienceHubPeriodicAssessmentRole)，该策略允许该 AWS Resilience Hub 服务担任预定评估的角色。

```
{
  "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"
      ]
    }
  ]
}
```

计划评测角色的信任策略（**AwsResilienceHubPeriodicAssessmentRole**）

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

跨账户设置

如果您在多个账户中使用 AWS 韧性监测中心，则需要使用以下 IAM 权限策略。根据您的用例，每个 AWS 账户可能需要不同的权限。在设置 AWS Resilience Hub 进行跨账户存取时，需要考虑以下账户和角色：

- 主账户 – AWS 您要在其中创建应用程序和运行评测的账户。
- 次要/资源 AWS 账户 — 资源所在的账户。

> **Note**
>
> - 使用基于角色的访问权限（使用上面提到的调用者角色）时，不需要执行此步骤。
> - 有关配置访问 Amazon Elastic Kubernetes Service 的权限的更多信息，请参阅 the section called “启用对您的 Amazon EKS 集群的 AWS Resilience Hub 访问权限”。

主账户设置

您必须在主账户AwsResilienceHubAdminAccountRole中创建一个新角色并允许 AWS Resilience Hub 访问权限才能代入该角色。此角色将用于访问您 AWS 账户中包含您的资源的另一个角色。它不应拥有读取资源的权限。

> **Note**
>
> - 角色名称必须为 AwsResilienceHubAdminAccountRole。
> - 它必须在主账户中创建。
> - 您当前的 IAM 用户/角色必须具有担任此角色的 iam:assumeRole 权限。
> - 替换 secondary_account_id_1/2/... 为相关的辅助账户标识符。

以下策略为您的角色提供访问 AWS 账户中其他角色的资源的执行者权限：

```
{
  {
  "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"
      ]
    }
```

```
  ]
}
```

管理员角色（AwsResilienceHubAdminAccountRole）的信任策略如下：

```
{
  "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"
    }
  ]
}
```

辅助/资源账户设置

在每个辅助账户中，您必须创建一个新的 AwsResilienceHubExecutorAccountRole 并启用以上创建的管理员角色以担任此角色。由于此角色将 AWS Resilience Hub 用于扫描和评估您的应用程序资源，因此还需要相应的权限。

但是，您必须将 AWSResilienceHubAsssessmentExecutionPolicy 托管式策略附加到角色，并附加执行者角色策略。

执行者角色信任策略如下所示：

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS 的托管策略 AWS Resilience Hub

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWSResilienceHubAsssessmentExecutionPolicy

您可以将 `AWSResilienceHubAsssessmentExecutionPolicy` 附加得到 IAM 身份。运行评估时，此策略向其他 AWS 服务授予执行评估的访问权限。

权限详细信息

该政策提供了足够的权限来向您的亚马逊简单存储服务 (Amazon S3) 存储桶发布警报 AWS FIS 和 SOP 模板。Amazon S3 存储桶的名称必须以 `aws-resilience-hub-artifacts-` 开头。如果您想发布到其他 Amazon S3 存储桶，则可以在调用 `CreateRecommendationTemplate` API 的同时执行此操作。有关更多信息，请参阅CreateRecommendationTemplate。

该策略包含以下权限：

- Amazon CloudWatch (CloudWatch)-获取您在亚马逊中为监控应用程序 CloudWatch 而设置的所有已实现警报。此外，我们还`cloudwatch:PutMetricData`用于发布`ResilienceHub`命名空间中应用程序的弹性分数 CloudWatch 指标。
- Amazon Data Lifecycle Manager — 获取并提供与您的 AWS 账户关联的亚马逊数据生命周期管理器资源的`Describe`权限。
- Amazon DevOps Guru — 列出与您的 AWS 账户关联的 Amazon DevOps Guru 资源并提供`Describe`权限。
- Amazon DynamoDB（DynamoDB）– 列出并提供与您的 AWS 账户关联的 Amazon DynamoDB 资源的 `Describe` 权限。
- Amazon ElastiCache (ElastiCache)-为与您的 AWS 账户关联的 ElastiCache 资源提供`Describe`权限。
- Amazon Elastic Compute Cloud（Amazon EC2）– 列出并提供与您的 AWS 账户关联的 Amazon EC2 资源的 `Describe` 权限。
- Amazon Elastic Container Registry (Amazon ECR) — 为与您的账户关联的亚马逊 ECR 资源提供`Describe`权限。 AWS
- 亚马逊弹性容器服务 (Amazon ECS) Servic `Describe` e — 为与 AWS 您的账户关联的亚马逊 ECS 资源提供权限。
- Amazon Elastic File System (Amazon EFS) — 为与您的 AWS 账户关联的亚马逊 EFS 资源提供`Describe`权限。
- Amazon Elastic Kubernetes Service（Amazon EKS）– 列出并提供与您的 AWS 账户关联的 Amazon EKS 资源的 `Describe` 权限。
- Amazon EC2 Auto Scaling — 列出与您的 AWS 账户关联的 Amazon EC2 Auto Scaling 资源并提供`Describe`权限。
- Amazon EC2 Systems Manager (SSM) — 为与您的 AWS 账户关联的 SSM 资源提供`Describe`权限。
- Amazon 故障注入服务 (AWS FIS) — 列出与您的 AWS 账户关联的 AWS FIS 实验和实验模板并提供`Describe`权限。
- 适用于 Windows File Server 的亚马逊 FSx（亚马逊 FSx）— 列出与`Describe`您的账户关联的亚马逊 FSx 资源并提供权限。 AWS
- Amazon RDS — 列出与您的 AWS 账户关联的 Amazon RDS 资源并为其提供`Describe`权限。
- Amazon Route 53（Route 53）– 列出与您的 AWS 账户关联的 Route 53 资源的 `Describe` 权限。
- Amazon Route 53 Resolver — 列出与您的 AWS 账户关联的 Amazon Route 53 Resolver 资源并为其提供`Describe`权限。

- Amazon Simple Notification Service（Amazon SNS）– 列出并提供与您 AWS 账户关联的 Amazon SNS 资源的 `Describe` 权限。
- Amazon Simple Queue Service（Amazon SQS）– 列出并提供与您的 AWS 账户关联的 Amazon SQS 资源的 `Describe` 权限。
- Amazon Simple Storage Service Amazon S3 – 列出并提供与您的 AWS 账户关联的 Amazon S3 资源的 `Describe` 权限。

> **Note**
>
> 运行评估时，如果托管策略中存在任何缺失的权限需要更新，则 AWS Resilience Hub 将使用 s3: GetBucketLogging 权限成功完成评估。但是， AWS Resilience Hub 将显示一条警告消息，列出缺少的权限，并提供添加权限的宽限期。如果您未在指定的宽限期内添加缺少的权限，则评估将失败。

- AWS Backup — 列出与您的 AWS 账户关联的 Amazon EC2 Auto Scaling 资源并获取其`Describe`权限。
- AWS CloudFormation — 列出与您的 AWS 账户关联的 AWS CloudFormation 堆栈上的资源并获取其`Describe`权限。
- AWS DataSync — 列出与您的 AWS 账户关联的 AWS DataSync 资源并为其提供`Describe`权限。
- AWS Directory Service — 列出与您的 AWS 账户关联的 AWS Directory Service 资源并为其提供`Describe`权限。
- AWS Elastic Disaster Recovery （弹性灾难恢复）— 为与您的 AWS 账户关联的 Elastic 灾难恢复资源提供`Describe`权限。
- AWS Lambda (Lambda) — 列出与您的账户关联的 Lambda 资源并为其提供`Describe`权限。 AWS
- AWS Resource Groups （Resource Groups）-列出与您的 AWS 账户关联的资源组资源并提供`Describe`权限。
- AWS Service Catalog （Service Catalog）— 列出与您的 AWS 账户关联的 Service Catalog 资源并提供`Describe`相应权限。
- AWS Step Functions — 列出与您的 AWS 账户关联的 AWS Step Functions 资源并为其提供`Describe`权限。
- Elastic Load Balancing — 列出与您的 AWS 账户关联的 Elastic Load Balancing 资源并提供`Describe`权限。
- `ssm:GetParametersByPath`— 我们使用此权限来管理为您的应用程序配置的 CloudWatch 警报、测试或 SOP。

AWS 账户需要以下 IAM 策略才能为用户、用户组和角色添加权限，从而为您的团队提供在运行评估时访问 AWS 服务的必要权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "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",
        "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:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
```

```
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "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:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "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": "*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET"
      ],
      "Resource": [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "ResilienceHub"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

AWS Resilience HubAWS 托管策略的更新

查看 AWS Resilience Hub 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面更改的自动提醒，请订阅 “ AWS Resilience Hub 文档历史记录” 页面上的 RSS feed。

更改	描述	日期
AWSResilienceHubAssessmentExecutionPolicy—AWS Resilience Hub 扩展了对适用于 Windows File Server 的亚马逊 FSx 的支持。	此 AWS Resilience Hub 策略允许您读取 Amazon FSx for Windows File Server 配置。	2024 年 3 月 26 日
AWSResilienceHubAssessmentExecutionPolicy—AWS Resilience Hub 扩展了对的支持 AWS Step Functions。	此 AWS Resilience Hub 策略允许您读取 AWS Step Functions 配置。	2023 年 10 月 30 日
AWSResilienceHubAssessmentExecutionPolicy – AWS Resilience Hub 改进对 Amazon Relational Database Service（Amazon RDS）的支持。	此 AWS Resilience Hub 策略允许您在运行评估时访问 Amazon RDS 上的资源。	2023 年 10 月 5 日
AWSResilienceHubAssessmentExecutionPolicy：新策略	此 AWS Resilience Hub 政策允许访问其他 AWS 服务以进行评估。	2023 年 6 月 26 日
AWS Resilience Hub 开始跟踪更改	AWS Resilience Hub 开始跟踪其 AWS 托管策略的更改。	2023 年 6 月 15 日

将 Terraform 状态文件导入 AWS Resilience Hub

AWS Resilience Hub 支持导入使用服务器端加密 (SSE)、亚马逊简单存储服务托管密钥 (SSE-S3) 或托管密钥 (SSE-KMS) 加密的 Terraform 状态文件。 AWS Key Management Service 如果您的 Terraform 状态文件使用客户提供的加密密钥（SSE-C）进行加密，则无法使用 AWS Resilience Hub 导入它们。

将 Terraform 状态文件导入到中 AWS Resilience Hub 需要以下 IAM 策略，具体取决于您的状态文件所在的位置。

从主账户中的 Amazon S3 存储桶导入 Terraform 状态文件

需要以下 Amazon S3 存储桶策略和 IAM policy 策略才能允许 AWS Resilience Hub 对位于主账户的 Amazon S3 存储桶中的 Terraform 状态文件进行读取。

- 存储桶策略 – 目标 Amazon S3 存储桶的存储桶策略，该存储桶位于主账户中。有关更多信息，请参阅以下示例。

```
{
  "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>"
    }
  ]
}
```

- 身份策略 — 为该应用程序定义的调用者角色或主 AWS 账户 AWS Resilience Hub 上的 AWS 当前 IAM 角色的关联身份策略。有关更多信息，请参阅以下示例。

```
{
  "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**
>
> 如果您使用的是 AWSResilienceHubAsssessmentExecutionPolicy 托管式策略，则不需要 ListBucket 权限。

> **Note**
>
> 如果您的 Terraform 状态文件使用 KMS 加密，则必须添加以下 kms:Decrypt 权限。

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

从位于辅助账户中的 Amazon S3 存储桶导入 Terraform 状态文件

- 存储桶策略 – 目标 Amazon S3 存储桶的存储桶策略，该存储桶位于其中一个辅助账户中。有关更多信息，请参阅以下示例。

```
{
 "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>"
    }
  ]
}
```

- 身份策略- AWS 账户角色的关联身份策略，该策略在主 AWS 账户 AWS Resilience Hub 上运行。有关更多信息，请参阅以下示例。

```
{
  "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**
>
> 如果您使用的是 AWSResilienceHubAsssessmentExecutionPolicy 托管式策略，则不需要 ListBucket 权限。

> **Note**
>
> 如果您的 Terraform 状态文件使用 KMS 加密，则必须添加以下 kms:Decrypt 权限。

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

允许 AWS Resilience Hub 访问您的亚马逊 Elastic Kubernetes Service 集群

AWS Resilience Hub 通过分析 Amazon EKS 集群的基础设施，评估亚马逊 Elastic Kubernetes Service (Amazon EKS) 集群的弹性。 AWS Resilience Hub 使用 Kubernetes 基于角色的访问控制 (RBAC) 配置来评估其他 Kubernetes (K8) 工作负载，这些工作负载是作为 Amazon EKS 集群的一部分部署的。 AWS Resilience Hub 要查询您的 Amazon EKS 集群以分析和评估工作负载，您必须完成以下操作：

- 在与 Amazon EKS 集群相同的账户中创建或使用现有 AWS Identity and Access Management (IAM) 角色。

- 允许 IAM 用户和角色访问您的 Amazon EKS 集群，并向 Amazon EKS 集群内的 K8s 资源授予额外的只读权限。有关允许 IAM 用户和角色访问您的 Amazon EKS 集群的更多信息，请参阅允许 IAM 用户和角色访问您的集群 - Amazon EKS。

Amazon EKS 控制面板运行的 AWS IAM Authenticator for Kubernetes 支持使用 IAM 实体访问集群。身份验证程序从 `aws-auth ConfigMap` 获取配置信息。

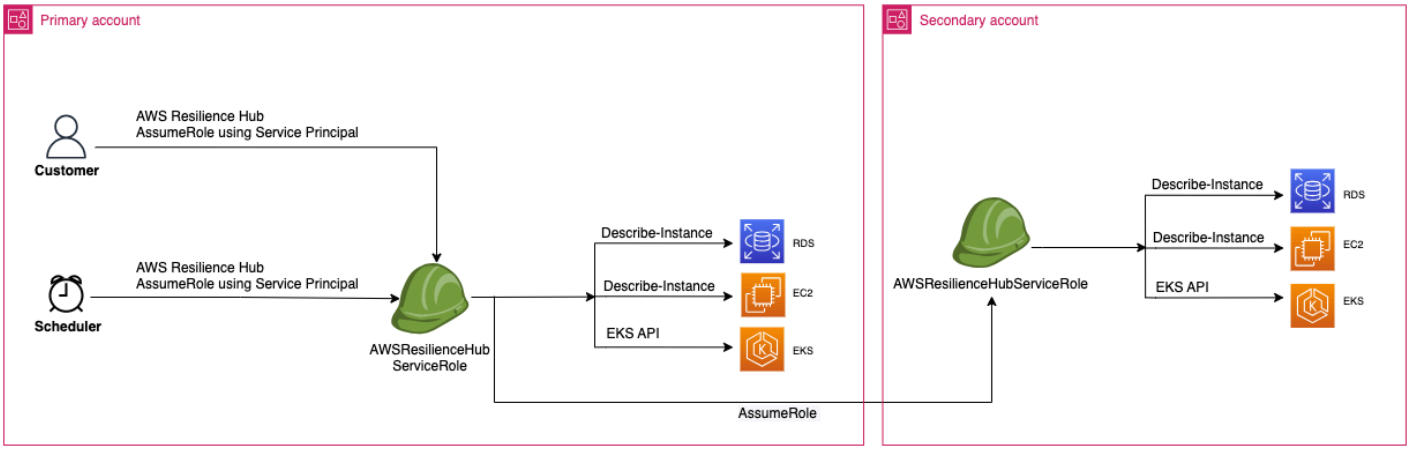
> **Note**
>
> - 有关所有`aws-auth ConfigMap`设置的更多信息，请参阅上的完整配置格式 GitHub。
> - 有关不同 IAM 实体的更多信息，请参阅 IAM 用户指南中的身份（用户、组和角色）。
> - 有关基于 Kubernetes 角色访问控制（RBAC）配置的更多信息，请参阅使用 RBAC 授权。

AWS Resilience Hub 使用您账户中的 IAM 角色查询 Amazon EKS 集群内的资源。 AWS Resilience Hub 要访问您的 Amazon EKS 集群中的资源， AWS Resilience Hub 必须将使用的 IAM 角色映射到对您的 Amazon EKS 集群内的资源具有足够只读权限的 Kubernetes 组。

AWS Resilience Hub 允许使用以下 IAM 角色选项之一访问您的 Amazon EKS 集群资源：

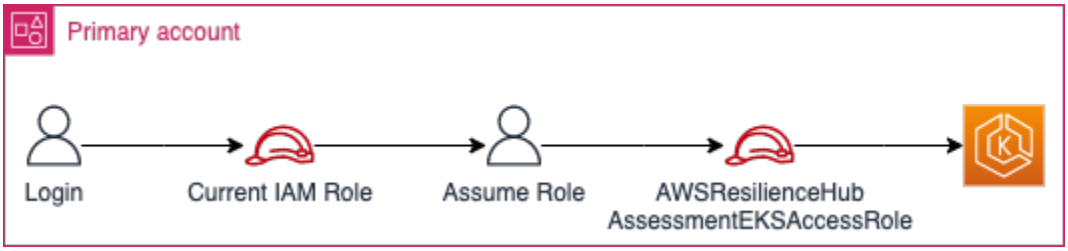
- 如果您的应用程序配置为使用基于角色的访问权限来访问资源，则在评测期间，将使用在创建应用程序时传递到 AWS Resilience Hub 的调用者角色或辅助账户角色访问您的 Amazon EKS 集群。

  以下概念图显示了将应用程序配置为基于角色的应用程序时如何 AWS Resilience Hub 访问 Amazon EKS 集群。

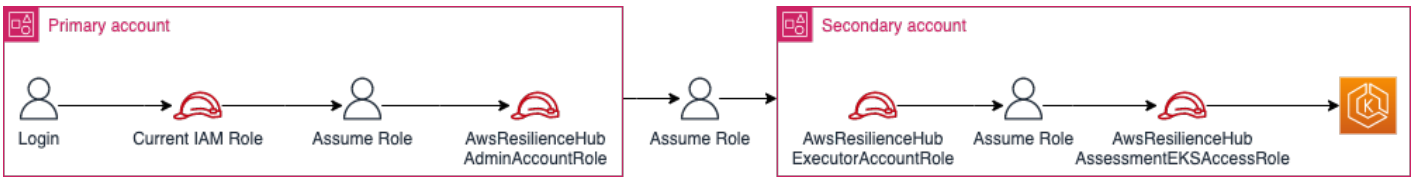


- 如果您的应用程序配置为使用当前 IAM 用户访问资源，则必须在与 Amazon EKS 集群相同的账户中创建一个名为 `AwsResilienceHubAssessmentEKSAccessRole` 的新的 IAM 角色。然后，此 IAM 角色将用于访问您的 Amazon EKS 集群。

  以下概念图显示了当应用程序配置为使用当前 IAM 用户权限时，如何 AWS Resilience Hub 访问部署在您的主账户中的 Amazon EKS 集群。



  以下概念图显示了当应用程序配置为使用当前 IAM 用户权限时，如何 AWS Resilience Hub 访问部署在辅助账户上的 Amazon EKS 集群。



授予对您的 Amazon EKS 集群中资源的 AWS Resilience Hub 访问权限

AWS Resilience Hub 允许您访问位于 Amazon EKS 集群上的资源，前提是您已配置所需的权限。

向授予发现和评估 Amazon EKS 集群内资源所需的权限 AWS Resilience Hub

1. 配置 IAM 角色以访问亚马逊 Amazon EKS 集群。

   如果您已使用基于角色的访问权限配置应用程序，则可以跳过此步骤，继续执行步骤 2，并使用创建应用程序时使用的角色。有关 AWS Resilience Hub 如何使用 IAM 角色的更多信息，请参阅 和 the section called “AWS 弹性中心如何与 IAM 配合使用”。

   如果您已使用当前 IAM 用户权限配置应用程序，则必须在与 Amazon EKS 集群相同的账户中创建 `AwsResilienceHubAssessmentEKSAccessRole` IAM 角色。然后，将在访问您的 Amazon EKS 集群时使用此 IAM 角色。

   在导入和评估您的应用程序时， AWS Resilience Hub 使用 IAM 角色访问您的 Amazon EKS 集群中的资源。此角色应在与您的 Amazon EKS 集群相同的账户中创建，并将与包含评估您的 Amazon EKS 集群所需的权限的 Kubernetes 组 AWS Resilience Hub 进行映射。

如果您的 Amazon EKS 集群与 AWS Resilience Hub 调用账户位于同一个账户中，则应使用以下 IAM 信任策略创建该角色。在此 IAM 信任策略中，`caller_IAM_role`用于在当前账户中调用 API AWS Resilience Hub。

> **Note**
>
> `caller_IAM_role`是与您的 AWS 用户账户关联的角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如果您的 Amazon EKS 集群位于跨账户（与 AWS Resilience Hub 调用账户不同的账户）中，则必须使用以下 `AwsResilienceHubAssessmentEKSAccessRole` IAM 信任策略创建 IAM 角色：

> **Note**
>
> 作为先决条件，要访问部署在与 AWS Resilience Hub 用户账户不同的账户中的 Amazon EKS 集群，您必须配置多账户访问权限。有关更多信息，请参阅

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/
AwsResilienceHubExecutorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 为 AWS Resilience Hub 应用程序创建`ClusterRole`和`ClusterRoleBinding`（或`RoleBinding`）角色。

   创建`ClusterRole`和`ClusterRoleBinding`并将授予分析和评估属于您的 AWS Resilience Hub Amazon EKS 集群中特定命名空间一部分的资源所需的只读权限。

   AWS Resilience Hub 允许您通过完成以下任一操作来限制其对命名空间的访问权限以生成弹性评估：

   a. 向 AWS Resilience Hub 应用程序授予跨所有命名空间的读取权限。

      AWS Resilience Hub 要评估 Amazon EKS 集群内所有命名空间中资源的弹性，您必须创建以下和。`ClusterRole` `ClusterRoleBinding`

      - `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — 定义评估您的 AWS Resilience Hub Amazon EKS 集群所需的权限。
      - `resilience-hub-eks-access-cluster-role-binding`（`ClusterRoleBinding`）– 在您的 Amazon EKS 集群中定义一个名为 `resilience-hub-eks-access-group` 的群组，向其用户授予在中 AWS Resilience Hub运行弹性评测所需的权限。

      向 AWS Resilience Hub 应用程序授予跨所有命名空间读取权限的模板如下：

```
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
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
```

```
  resources:
    - awsnodetemplates
  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. 授 AWS Resilience Hub 予读取特定命名空间的权限。

您可以使用限制 AWS Resilience Hub 访问一组特定命名空间内的资源。RoleBinding要实现此目的，您必须创建以下角色：

- ClusterRole— AWS Resilience Hub 要访问 Amazon EKS 集群中特定命名空间中的资源并评估其弹性，您必须创建以下角色。ClusterRole
  - resilience-hub-eks-access-cluster-role – 指定评测特定命名空间内资源的必要权限。
  - resilience-hub-eks-access-global-cluster-role— 指定在您的 Amazon EKS 集群中评估集群范围内的资源（这些资源与特定命名空间无关）所需的权限。 AWS Resilience Hub 需要访问您的 Amazon EKS 集群上集群范围的资源（例如节点）的权限，以评估您的应用程序的弹性。

  创建 ClusterRole 角色的模板如下：

```
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
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
    verbs:
      - get
      - list

---
EOF
```

- RoleBinding角色-此角色授予 AWS Resilience Hub 访问特定命名空间内资源所需的权限。也就是说，您必须在每个命名空间中创建RoleBinding角色 AWS Resilience Hub 才能访问给定命名空间内的资源。

> **Note**
>
> 如果您将 ClusterAutoscaler 用于自动扩展，则您必须另外在 kube-system 中创建 RoleBinding。这是评测您的 ClusterAutoscaler 所必需的（它是 kube-system 命名空间的一部分）。
> 通过这样做，您将授予 AWS Resilience Hub 评估kube-system命名空间内资源所需的权限，同时评估您的 Amazon EKS 集群。

创建 RoleBinding 角色的模板如下：

```
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角色-此角色授予访问集群范围 AWS Resilience Hub 的资源所需的权限。

  创建 ClusterRoleBinding 角色的模板如下：

```
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. 更新 aws-auth ConfigMap 以将 resilience-hub-eks-access-group 与用于访问 Amazon EKS 集群的 IAM 角色进行映射。

   此步骤在步骤 1 中使用的 IAM 角色与步骤 2 中创建的 Kubernetes 组之间创建映射。此映射向 IAM 角色授予访问 Amazon EKS 集群内资源的权限。

   > **Note**
   >
   > - ROLE-NAME 指用于访问 Amazon EKS 集群的 IAM 角色。
   >   - 如果您的应用程序配置为使用基于角色的访问权限，则该角色应为创建应用程序 AWS Resilience Hub 时传递的调用者角色或辅助账户角色。
   >   - 如果您的应用程序配置为使用当前 IAM 用户访问资源，则该用户必须是 AwsResilienceHubAssessmentEKSAccessRole。
   > - ACCOUNT-ID应该是 Amazon EKS 集群的 AWS 账户 ID。

   您可以通过以下方式之一创建 aws-auth ConfigMap：

   - 使用 eksctl

     运行以下命令以更新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
     ```

   - 您可以通过将 IAM 角色详细信息添加到数据下的 ConfigMap 的 mapRoles 部分来手动编辑 aws-auth ConfigMap。要编辑aws-auth ConfigMap ，请键入以下命令。

     ```
     kubectl edit -n kube-system configmap/aws-auth
     ```

     mapRoles 部分可能包括以下参数：

     - rolearn（IAM）角色的 Amazon 资源名称（ARN）。

  - ARN 语法 – `arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`。
- `username` – Kubernetes 内要映射到 IAM 角色的用户名。`AwsResilienceHubAssessmentEKSAccessRole`
- `groups` – 群组名称应与步骤 2（`resilience-hub-eks-access-group`）中创建的群组名称相匹配。

> **Note**
>
> 如果 `mapRoles` 部分不存在，则必须手动添加此部分。

使用以下模板将 IAM 角色详细信息添加到数据下的 `ConfigMap` 的 `mapRoles` 部分。

```
    - groups:
      - resilience-hub-eks-access-group
      rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
      username: AwsResilienceHubAssessmentEKSAccessRole
```

允许发布 AWS Resilience Hub 到您的 Amazon 简单通知服务主题

本节介绍如何启用 AWS Resilience Hub 向您的亚马逊简单通知服务 (Amazon SNS) Simple SNS Service 主题发布有关该应用程序的通知。要向 Amazon SNS 主题推送通知，请确保您具备以下条件：

- 一个活跃的 AWS Resilience Hub 应用程序。
- AWS Resilience Hub 必须向其发送通知的现有 Amazon SNS 主题。有关创建 Amazon SNS 主题的信息，请参阅创建 Amazon SNS 主题。

AWS Resilience Hub 要允许向您的 Amazon SNS 主题发布通知，您必须使用以下内容更新 Amazon SNS 主题的访问策略：

```
{
  "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**
>
> 当您使用 AWS Resilience Hub 将来自可选区域的消息发布到位于默认启用的区域中的主题时，您必须修改为 Amazon SNS 主题创建的资源策略。将主体的值从 `resiliencehub.amazonaws.com` 更改为 `resiliencehub.<opt-in-region>.amazonaws.com`。

如果您使用的是服务器端加密（SSE）Amazon SNS 主题，则必须确保 AWS Resilience Hub 具有对 Amazon SNS 加密密钥的 `Decrypt` 和 `GenerateDataKey*` 访问权限。

要提供`Decrypt`和`GenerateDataKey*`访问权限 AWS Resilience Hub，您必须在 AWS Key Management Service 访问策略中包含以下权限。

```
{
  "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"
    }
  ]
}
```

限制包含或排除 AWS Resilience Hub 推荐的权限

AWS Resilience Hub 允许您限制每个应用程序包含或排除推荐的权限。您可以使用以下 IAM 信任策略限制每个应用程序包含或排除建议的权限。在此 IAM 信任策略中，`caller_IAM_role`（与您的 AWS 用户账户关联）用于当前账户中调用 API 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"
    }
  ]
}
```

中的基础设施安全 AWS Resilience Hub

作为一项托管服务，AWS Resilience Hub 受到《Amazon Web Services：安全流程概述》白皮书中描述的 AWS 全球网络安全程序的保护。

您可以使用 AWS 已发布的 API 调用 AWS Resilience Hub 通过网络进行访问。客户端必须支持传输层安全性（TLS）1.2 或更高版本。建议使用 TLS 1.3 或更高版本。客户端还必须支持具有完全向前保密（PFS）的密码套件，例如 Ephemeral Diffie-Hellman（DHE）或 Elliptic Curve Ephemeral Diffie-Hellman（ECDHE）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

使用其他服务

本节介绍与之交互的 AWS 服务 AWS Resilience Hub。

主题

- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- AWS Trusted Advisor

AWS CloudFormation

AWS Resilience Hub 与 AWS CloudFormation 集成，后者是一项服务，可帮助您对 AWS 资源进行建模和设置，这样您只需花较少的时间来创建和管理资源与基础设施。您可以创建一个模板，描述您所需的所有 AWS 资源（例如 AWS::ResilienceHub:::ResiliencyPolicy 和 AWS::ResilienceHub:::App）、AWS CloudFormation 预置和配置这些资源。

在您使用 AWS CloudFormation 时，可重复使用您的模板来不断地重复设置您的 AWS Resilience Hub 资源。仅描述您的资源一次，然后在多个AWS账户和区域中反复配置相同的资源。

AWS Resilience Hub 和 AWS CloudFormation 模板

要为 AWS Resilience Hub 和相关服务设置和配置资源，您必须了解 AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述要在 AWS CloudFormation 堆栈中调配的资源。如果您不熟悉 JSON 或 YAML，可以在 AWS CloudFormation Designer 的帮助下开始使用 AWS CloudFormation 模板。有关更多信息，请参阅 AWS CloudFormation 用户指南中的什么是 AWS CloudFormation Designer？。

AWS Resilience Hub 支持在 AWS CloudFormation 中创建 AWS:: ResilienceHub::: ResiliencePolicy 和 AWS:: ResilienceHub::: App。有关更多信息（包括 AWS::ResilienceHub:::ResiliencyPolicy 和 AWS::ResilienceHub:::App 的 JSON 和 YAML 模板示例），请参阅 AWS CloudFormation 用户指南中的 AWS Resilience Hub 资源类型参考。

您可以使用 AWS CloudFormation 堆栈来定义 AWS Resilience Hub 应用程序。堆栈允许您将相关资源作为单个单元进行管理。某个堆栈可能包含运行 Web 应用程序所需的所有资源，如 Web 服务器或联网规则。

了解有关 AWS CloudFormation 的更多信息

有关 AWS CloudFormation 的更多信息，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API 参考
- AWS CloudFormation 命令行界面用户指南

AWS CloudTrail

AWS Resilience Hub 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在中执行的操作的记录 AWS Resilience Hub。 CloudTrail 将所有 API 调用捕获 AWS Resilience Hub 为事件。捕获的调用包括来自 AWS Resilience Hub 控制台的调用和对 AWS Resilience Hub API 操作的代码调用。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件 AWS Resilience Hub。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的事件历史记录中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 AWS Resilience Hub、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关的更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

AWS Systems Manager

AWS Resilience Hub 与 Systems Manager 合作，通过提供大量可用作这些 SOP 基础的 SSM 文档，自动执行 SOP 的步骤。

AWS Resilience Hub 为您提供了包含运行不同 Systems Manager 文档所需的 IAM 角色的 AWS CloudFormation 模板，每个文档一个角色具有特定文档所需的权限。使用 AWS CloudFormation 模板创建堆栈后，它将设置 IAM 角色并将元数据保存在 Systems Manager 参数中，以便 Systems Manager 自动化文档在不同的恢复过程中运行。

有关使用 SOP 的更多信息，请参阅 标准操作流程。

AWS Trusted Advisor

AWS Trusted Advisor 是 AWS 最佳实践建议的集中库，可帮助您识别、确定优先级并优化部署 AWS。 AWS Trusted Advisor 检查您的 AWS 环境，然后在有机会节省资金、提高系统可用性和性能

或帮助填补安全漏洞时通过检查提出建议。这些支票根据其目的分为多个类别。有关不同类别的登机手续的更多信息 AWS Trusted Advisor，请参阅《AWS Support用户指南》。

AWS Trusted Advisor 通过对容错类别 AWS Resilience Hub 下的每个应用程序进行弹性检查，提供多项高级弹性建议。容错类别列出了测试应用程序以确定其弹性和可靠性的所有检查。当存在可能导致弹性风险并影响应用程序可用性以实现业务连续性的 AppComponent 故障和违反策略时，这些检查会提醒您。它还在 “建议的行动” 部分中提供了弹性建议，这些建议将提高降低这些风险的机会，该部分需要在中 AWS Resilience Hub讨论。有关中针对每个应用程序的建议的更多见解 AWS Trusted Advisor，我们建议您查看中提供的详细建议 AWS Resilience Hub。

AWS Trusted Advisor 为中的每个应用程序提供了以下检查 AWS Resilience Hub：

- AWS Resilience Hub 应用程序弹性分数 — 根据应用程序的最新评估检查其弹性分数，如果应用程序的 AWS Resilience Hub 弹性分数低于特定值，则会提醒您。

  警报标准

  - 绿色-表示您的应用程序的弹性分数为 70 及以上。
  - 黄色-表示您的应用程序的弹性分数介于 40 和 69 之间。
  - 红色-表示您的应用程序的弹性分数低于 40。

  建议的行动

  要改善应用程序的弹性状况并获得尽可能高的弹性分数，请使用应用程序资源的最新更新版本进行评估，并在适用的情况下实施建议的操作建议。有关运行、审查和实施评估、审查和包含/排除操作建议以及实施这些建议的更多信息，请参阅以下主题：

  - the section called “运行弹性评估”
  - the section called “查看评估报告”
  - the section called “查看弹性建议”
  - the section called “包含或排除操作建议”
- AWS Resilience Hub 违反应用程序策略-检查应用程序是否符合您为 AWS Resilience Hub 应用程序设置的 RTO 和 RPO 目标，并在应用程序未达到 RTO 和 RPO 目标时向您发出警报。

  警报标准

  - 绿色 — 表示应用程序有策略，估计的工作负载 RTO 和估计的工作负载 RPO 达到 RTO 和 RPO 目标。
  - 黄色-表示该应用程序有策略且尚未经过评估。

- 红色 — 表示应用程序有策略，且估计的工作负载 RTO 和估计的工作负载 RPO 未达到 RTO 和 RPO 目标。

  建议的行动

  为确保应用程序的估计工作负载 RTO 和估计的工作负载 RPO 仍然符合定义的 RTO 和 RPO 目标，请定期使用应用程序资源的最新更新版本进行评估。此外，如果您想确保应用程序的弹性政策不会被违反，我们建议您查看评估报告并实施建议的弹性建议。有关启用 AWS Resilience Hub 每天代表您运行评估、运行评估、查看弹性建议以及实施这些建议的更多信息，请参阅以下主题：

  - the section called “编辑应用程序资源”（ AWS Resilience Hub 要允许您每天运行评估，请完成更新应用程序程序的弹性偏差检测中的步骤，选中 “每天自动评估此应用程序” 复选框。 ）
  - the section called “运行弹性评估”
  - the section called “查看评估报告”
  - the section called “查看弹性建议”
  - the section called “包含或排除操作建议”

- AWS Resilience Hub 应用程序评估年限 — 检查自您上次对每个应用程序进行评估以来的时间 AWS Resilience Hub。如果您在指定的天数内没有运行评测，则会向您发出警报。

  警报标准

  - 绿色-表示您在过去 30 天内对应用程序进行了评估。
  - 黄色-表示您在过去 30 天内没有对应用程序进行评估。

  建议的行动

  定期运行评估，以管理和改善应用程序的弹性状况 AWS。如果您 AWS Resilience Hub 想代表您每天评估您的应用程序，则可以通过在 AWS Resilience Hub 弹性偏差检测中选中 “每天自动评估此应用程序” 复选框来启用该应用程序。要选中 “每天自动评估此应用程序” 复选框，请在中填写 “更新应用程序的弹性偏差检测”。???

  > **Note**
  >
  > 该检查仅确定那些至少接受过一次评估的申请的评估年龄。 AWS Resilience Hub

- AWS Resilience Hub 应用程序组件检查-检查应用程序中的应用程序组件 (AppComponent) 是否不可恢复。也就是说，如果在发生中断事件时仍 AppComponent 无法恢复，则可能会出现未知的数据丢失和系统停机。如果警报条件设置为红色， AppComponent 则表示无法恢复。

建议的行动

为确保您的 AppComponent 可恢复，请查看并实施弹性建议，然后进行新的评估。有关查看弹性建议的更多信息，请参阅the section called “查看弹性建议”。

有关使用的更多信息 AWS Trusted Advisor，请参阅《AWS Support用户指南》。

《AWS Resilience Hub 用户指南》的文档历史记录

下表描述了此版本的文档 AWS Resilience Hub。

- API 版本：最新
- 最新文档更新：2024 年 3 月 28 日

变更	说明	日期
AWS Trusted Advisor 增强	AWS Resilience Hub AWS Trusted Advisor 通过添加检查来识别不可恢复的应用程序组件（ ）AppComponents，扩展了对的支持。 有关更多信息，请参阅 the section called “AWS Trusted Advisor”。	2024 年 3 月 28 日
AWS Resilience Hub 扩展了对推荐警报的支持	AWS Resilience Hub 已使用允许您创建 AWS Resilience Hub 内部 AWS （例如 Amazon CloudWatch）或外部推荐的警报的值更新了`README.md` 模板文件 AWS。 有关更多信息，请参阅 the section called “管理警报”。	2024 年 3 月 26 日
AWS Resilience Hub 扩展了对适用于 Windows File Server 的亚马逊 FSx 的支持	AWS Resilience Hub 扩展了对 Amazon FSx for Windows File Server 资源的评估支持，同时评估应用程序的弹性。对于使用 Amazon FSx for Windows File Server 的应用程序 AWS Resilience Hub ，提供了一套新的弹性建议，涵	2024 年 3 月 26 日

	盖可用区 (AZ) 和多可用区部署、备份计划以及数据复制。 AWS Resilience Hub 支持适用于 Windows File Server 的 Amazon FSx，包括对微软 Active Directory 的文件系统依赖，用于区域内和跨区域部署。 有关更多信息，请参阅以下主题： • the section called “支持的 AWS Resilience Hub 资源” • the section called “AWSResilienceHubAsssessmentExecutionPolicy” • the section called “将资源分组为 AppComponent”	
AWS Resilience Hub 提供了有关弹性分数的更多信息	AWS Resilience Hub 更新了 Resiliency 分数用户体验，以帮助您轻松浏览和了解改善应用程序弹性状况所需的操作。 有关更多信息，请参阅 the section called “了解弹性分数”。	2023 年 11 月 9 日

AWS Resilience Hub 扩展了对包含亚马逊 Elastic Kubernetes Service (Amazon EKS) 资源的应用程序的支持	AWS Resilience Hub 扩展了对包含 Amazon EKS 资源的应用程序的支持，以包括新的操作建议。在运行包含来自 Amazon EKS 集群的资源的评估时，我们现在将建议实施测试和警报，以帮助提高应用程序的弹性状态。 有关更多信息，请参阅 the section called “Amazon 错误注入服务实验”。	2023 年 11 月 9 日
AWS Resilience Hub 提供了应用程序级别的更多信息	AWS Resilience Hub 在应用程序级别提供了有关估计工作负载 RTO 和估计工作负载 RPO 的其他信息。此其他信息显示了根据最新成功评估得出的应用程序可能的最大估计的工作负载 RTO 和估计的工作负载 RPO。此值是所有中断类型的最大估计的工作负载 RTO 和估计的工作负载 RPO。 有关更多信息，请参阅 the section called “应用程序”。	2023 年 10 月 30 日

AWS Resilience Hub 扩展对 AWS Step Functions 资源的评估支持	AWS Resilience Hub 扩展对 AWS Step Functions 资源的评估支持，同时评估应用程序的弹性。 AWS Resilience Hub 分析 AWS Step Functions 配置，包括状态机类型（标准或快速工作流程）。此外，AWS Resilience Hub 还将提供建议，帮助您实现预计的工作负载恢复时间目标 (RTO) 和预计的工作负载恢复点目标 (RPO)。要评估包括 AWS Step Functions 资源在内的应用程序，必须使用 AWS 托管策略或手动添加允许 AWS Resilience Hub 读取 AWS Step Functions 配置的特定权限来设置必要的权限。 有关这些权限的更多信息，请参阅 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 10 月 30 日

AWS Resilience Hub 允许排除操作建议	AWS Resilience Hub 允许您排除操作建议，包括警报、标准操作程序 (SOP) 和 Amazon 故障注入服务 (AWS FIS) 测试。在对进行评估时 AWS Resilience Hub，将为您提供估计的恢复时间以及有关提高所评估应用程序弹性的方法的建议。使用排除推荐工作流程，您现在可以排除与其无关的推荐警报、SOP 和 AWS FIS 测试。如果您使用的平台不是建议的平台，或者已经在其他方法中实施了建议，则排除工作流非常有用。 有关更多信息，请参阅以下主题： • the section called “包含或排除操作建议” • the section called “限制包含或排除 AWS Resilience Hub 建议的权限”	2023 年 8 月 9 日

改进权限设计 AWS Resilience Hub	AWS Resilience Hub 引入了新的权限设计，以便在为配置 AWS Identity and Access Management (IAM) 角色时提供灵活性 AWS Resilience Hub。它还将权限整合到单个角色中，能够创建对您和您的团队有意义的自定义角色名称。中的新托管策略 AWS Resilience Hub 将允许您对支持的服务拥有相应的权限。如果您对当前的权限设置方法感到满意，我们将继续支持手动配置。 有关 AWS 托管策略的更多信息，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 8 月 2 日

应用程序弹性漂移检测 AWS Resilience Hub	AWS Resilience Hub 允许您主动检测和了解解决应用程序弹性问题的必要措施。在估计的工作负载恢复时间目标（RTO）或估计的工作负载恢复点目标（RPO）从达到目标变为不再满足贵组织的业务目标时，允许 Amazon Simple Notification Service（Amazon SNS）收到通知。从手动运行评估时被动地发现弹性问题，转变为通过 Amazon SNS 主题主动收到通知，这将使您能够更早地预测潜在的中断，并为实现恢复目标提供额外的信心。 有关更多信息，请参阅以下主题： • the section called “步骤 5：设置弹性偏差检测” • the section called “编辑应用程序资源”	2023 年 8 月 2 日

AWS Resilience Hub 改进了对亚马逊 Relational Database Service 和亚马逊 Aurora 的支持	AWS Resilience Hub 扩展了对 Amazon Relational Database Service 代理、Headless 和 Amazon Aurora 数据库配置的评估支持。此外，在评估包含 Amazon RDS 的应用程序时，我们现在将区分不同的数据库引擎，以提供更精确的估计工作负载恢复时间目标 (RTO)。AWS Resilience Hub 还将提供其他措施，以便在您的 AWS 环境中实施弹性最佳实践。最佳实践可以包括使用 DevOps Guru for Amazon RDS 的性能见解、增强的监控以及在支持的数据库引擎上实现蓝/绿部署自动化。 要详细了解将所有受支持服务的资源纳入评估所需的权限，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。AWS Resilience Hub	2023 年 8 月 2 日

AWS Resilience Hub 扩展了对 Amazon 弹性区块存储快照的支持	AWS Resilience Hub 扩展了对亚马逊 Elastic Block Store (Amazon EBS) Store 的评估支持，以识别亚马逊 EBS 快照，这些快照是在同一个亚马逊 EBS 区域使用直接 API 拍摄的。除了目前为使用亚马逊数据生命周期管理器（Amazon Data Lifecycle Manager）或 AWS Backup的客户提供的支持之外，还提供了扩展支持。 有关更多信息，请参阅 Amazon Elastic Block Store（Amazon EBS)。	2023 年 8 月 2 日

Amazon Elastic Compute Cloud 增强功能	AWS Resilience Hub 扩大了对亚马逊弹性计算云 (Amazon EC2) 的支持。对于不同大小的应用程序，AWS 允许使用 Amazon EC2 的客户选择适合其用例的配置。 AWS Resilience Hub 支持对以下 Amazon EC2 配置进行评估： • 按需型实例。 • 实例由 AWS Backup 和备份 AWS Elastic Disaster Recovery。 • 支持 Amazon Route 53 应用程序恢复控制器（Route 53 ARC）的自动扩缩组 展望未来，评估支持将扩展到包括竞价型实例、专属主机、专用实例、置放群组和实例集。 有关更多信息，请参阅 the section called “AWS Resilience Hub 访问权限参考”。	2023 年 6 月 27 日
AWS 托管策略更新	添加了一项新策略，允许访问其他 AWS 服务以执行评估。 有关更多信息，请参阅 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 6 月 26 日

新的 Amazon DynamoDB 操作建议警报	对于使用 Amazon DynamoDB 的应用程序 AWS Resilience Hub ，现在提供了一组新的警报，提醒您注意按需和预配置容量模式以及全局表的弹性风险。要访问新警报，您可能需要更新所用角色的 AWS Identity and Access Management (IAM) 策略。 有关更多信息，请参阅 the section called “AWS Resilience Hub 访问权限参考”。	2023 年 5 月 2 日
AWS Trusted Advisor 增强	AWS Resilience Hub 扩展了对 AWS Trusted Advisor 使用 Amazon DynamoDB 的应用程序的支持。当你 AWS Trusted Advisor 与一起使用时 AWS Resilience Hub，你现在可以在过去 30 天内未对应用程序进行评估时收到通知。此通知会提示您重新评估应用程序，以了解是否有任何更改会影响其弹性。 有关 AWS Resilience Hub 评估期限检查的更多信息，请参阅 the section called “AWS Trusted Advisor”。	2023 年 5 月 2 日

额外支持 Amazon Simple Storage Service	除了目前支持亚马逊简单存储服务 (Amazon S3) Simple S3 跨区域复制 (Amazon S3 CRR) /亚马逊S3同区域复制 (SRR)、版本控制和备份外，AWS Resilience Hub 现在还将评估亚马逊S3的多区域接入点 AWS 、亚马逊S3复制时间控制 (Amazon S3 RTC) 和备份恢复 (PITR) 配置。 AWS point-in-time 有关更多信息，请参阅以下主题： • the section called “AWS Resilience Hub 访问权限参考” • 管理您的 Amazon S3 存储	2023 年 3 月 21 日

额外支持 Amazon Elastic Kubernetes Service	AWS Resilience Hub 已将 Amazon EKS 集群添加为用于定义、验证和跟踪应用程序弹性的支持资源。客户可以将 Amazon EKS 集群添加到新的或现有的应用程序中，并获得有关提高弹性的评估和建议。客户可以使用 AWS CloudFormation、Terraform、和添加应用程序资源。 AWS Resource Groups AppRegistry此外，客户可以在一个或多个区域中直接添加一个或多个 Amazon EKS 集群，每个集群中都有一个或多个命名空间。这 AWS Resilience Hub 允许提供单一和跨区域的评估和建议。除了检查部署外，副本和 Pod AWS Resilience Hub 还将分析集群的整体弹性。 ReplicationControllers AWS Resilience Hub 支持无状态 Amazon EKS 集群工作负载。这些新功能在所有受支持的 AWS 地区 AWS Resilience Hub 都可用。 有关更多信息，请参阅以下主题： • the section called “步骤 2：管理您的应用程序资源” • the section called “添加 EKS 集群”	2023 年 3 月 21 日

	• the section called “AWS Resilience Hub 访问权限参考” • AWS 区域服务	
额外支持 Amazon Elastic File System	除了目前对亚马逊弹性文件系统（Amazon EFS）备份的支持外，现在 AWS Resilience Hub 还将评估亚马逊 EFS 的亚马逊 EFS 复制和可用区配置。 有关更多信息，请参阅以下主题： • the section called “支持的 AWS Resilience Hub 资源” • 什么是 Amazon Elastic File System？	2023 年 3 月 21 日
支持应用程序输入源	AWS Resilience Hub 现在可以透明地了解您的应用程序来源。这可以帮助您添加、删除和重新导入应用程序的输入源，并发布新的应用程序版本。 有关更多信息，请参阅 the section called “编辑应用程序资源”。	2023 年 2 月 21 日

支持应用程序配置参数	AWS Resilience Hub 现在提供了一种输入机制，用于收集有关与您的应用程序关联的资源的其他信息。利用这些信息，AWS Resilience Hub 将更深入地了解您的资源并提供更好的弹性建议。 有关更多信息，请参阅以下主题： • the section called “应用程序配置参数” • the section called “步骤 7：配置应用程序配置参数” • the section called “更新应用程序配置参数”	2023 年 2 月 21 日
额外支持 Amazon Elastic Block Store	除了目前对亚马逊弹性区块存储（Amazon EBS）卷的支持外 AWS Resilience Hub ，现在还将通过亚马逊数据生命周期管理器和亚马逊EBS快速快照恢复（FSR）评估亚马逊EBS快照。 有关更多信息，请参阅以下主题： • the section called “AWS Resilience Hub 访问权限参考” • Amazon Elastic Block Store（Amazon EBS)	2023 年 2 月 21 日

与集成 AWS Trusted Advisor	AWS Trusted Advisor 用户将能够查看已通过评估的与其帐户关联的应用程序 AWS Resilience Hub。 AWS Trusted Advisor 显示最新的弹性分数，并提供表明是否满足目标弹性策略（RTO 和 RPO）的状态。每次运行评估时，都会 AWS Resilience Hub 更新 AWS Trusted Advisor 最新结果。 AWS Trusted Advisor 是一项持续分析您的 AWS 账户并提供建议以帮助您遵循 AWS 最佳实践和 Well-Architect AWS ed 指南的服务。 有关更多信息，请参阅 the section called “AWS Trusted Advisor”。	2022 年 11 月 18 日

支持 Amazon Simple Notification Service（Amazon SNS）	AWS Resilience Hub 现在，通过分析 Amazon SNS 配置（包括订阅者）来评估使用 Amazon SNS 的应用程序，并提供建议，以满足组织为应用程序设定的预计工作负载恢复目标（估计的工作负载 RTO 和估计的工作负载 RPO）。Amazon SNS 是一项托管服务，可将消息从发布者（创建者）传输给订阅用户（使用者）。 有关更多信息，请参阅以下主题： • the section called “支持的 AWS Resilience Hub 资源” • the section called “Identity and Access Management” • the section called “将资源分组为 AppComponent”	2022 年 11 月 16 日

额外支持 Amazon Route 53 应用程序恢复控制器（Amazon Route 53 ARC）	AWS Resilience Hub 现在正在评估亚马逊 Route 53 ARC 的 Elastic Load Balancing 和亚马逊关系数据库服务（Amazon RDS），其中包括就亚马逊 Route 53 ARC 何时有益提供建议。将亚马逊 Route 53 ARC 评估支持扩展到 AWS Resilience Hub了 A AWS uto Scaling Group (AWS ASG) 和亚马逊 DynamoDB 之外。Amazon Route 53 ARC 为您的应用程序提供高可用性，允许您快速将整个应用程序失效转移到失效转移区域。 有关更多信息，请参阅以下主题： • the section called “支持的 AWS Resilience Hub 资源” • the section called “Identity and Access Management”	2022 年 11 月 16 日

对 AWS Backup 的额外支持	AWS Resilience Hub 现在正在评估亚马逊 Route 53 ARC 的 Elastic Load Balancing 和亚马逊关系数据库服务（Amazon RDS），其中包括就亚马逊 Route 53 ARC 何时有益提供建议。将亚马逊 Route 53 ARC 评估支持扩展到 AWS Resilience Hub了 A AWS uto Scaling Group (AWS ASG) 和亚马逊 DynamoDB 之外。Amazon Route 53 ARC 为您的应用程序提供高可用性，允许您快速将整个应用程序失效转移到失效转移区域。 有关更多信息，请参阅以下主题： • the section called “支持的 AWS Resilience Hub 资源” • the section called “Identity and Access Management”	2022 年 11 月 16 日
更新内容：添加了新的应用程序组件资源	将 Route53 AWS 和 Backup 添加到 AppComponent 分组部分支持的应用程序组件资源列表中。	2022 年 7 月 1 日
新内容：应用程序合规性状态概念	添加了“检测到更改”状态类型。	2022 年 6 月 2 日

简介 AWS Resilience Hub	AWS Resilience Hub 现已上市。本指南介绍 AWS Resilience Hub 如何使用分析基础架构、获取提高 AWS 应用程序弹性的建议、查看弹性分数等。	2021 年 11 月 10 日

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。