aws

用户指南

AWS Resilience Hub

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Resilience Hub: 用户指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

AWS Resilience Hub 1
什么是 AWS Resilience Hub? 1
AWS Resilience Hub — 弹性管理 2
AWS Resilience Hub — 弹性测试 4
AWS Resilience Hub 概念 5
AWS Resilience Hub 表象人格 8
支持的 AWS Resilience Hub 资源 9
AWS Resilience Hub 和 “我的应用程序” 13
开始使用 14
先决条件 14
添加应用程序 15
使用 AWS Resilience Hub 26
AWS Resilience Hub 摘要 27
AWS Resilience Hub 仪表板 31
管理 应用程序 32
管理弹性策略 54
在中管理弹性评估 AWS Resilience Hub 59
通过弹性小工具管理弹性评估 68
管理警报 71
管理标准操作程序 76
管理 AWS Fault Injection Service 实验 81
了解弹性分数 89
将建议集成到应用程序中 100
使用 AWS Resilience Hub API 描述和管理应用程序 106
准备应用程序 106
运行和分析应用程序 112
修改您的应用程序 130
安全性 134
数据保护 135
身份和访问管理 136
基础结构安全性 183
AWS 服务的弹性检查 183
Amazon Elastic File System 184
亚马逊关系数据库服务和亚马逊 Aurora 184

Amazon Simple Storage Service 186
Amazon DynamoDB 187
Amazon Elastic Compute Cloud 187
Amazon EBS 188
AWS Lambda 189
Amazon Elastic Kubernetes Service 189
Amazon Simple Notification Service 190
Amazon Simple Queue Service 190
Amazon Elastic Container Service 190
Elastic Load Balancing 191
Amazon API Gateway 191
Amazon DocumentDB 191
NAT 网关 192
Amazon Route 53 192
Amazon 应用程序恢复控制器（ARC） 192
适用于 Windows File Server 的 Amazon FSx 193
AWS Step Functions 193
亚马逊 ElastiCache （Redis OSS） 193
使用其他服务 195
AWS CloudFormation 195
AWS CloudTrail 196
AWS Systems Manager 196
AWS Trusted Advisor 196
文档历史记录 199
下一代弹性中心 226
什么是下一代弹性中心？ 226
关键功能一览 226
支持的区域和可用性 227
定价概览 228
相关服务 229
设置下一代弹性中心 229
先决条件 229
所需的 IAM 权限和角色 230
AWS 托管策略 236
配置 AWS 组织集成（可选） 244
Multi-account 设置（没有 AWS 组织） 245

Customer-managed 密钥（可选） 247
下一代弹性中心入门 247
教程概述和先决条件 248
步骤 1：配置弹性策略 249
第 2 步：创建您的第一个系统和服务 249
第 3 步：进行首次故障模式评估 251
第 4 步：查看故障模式的调查结果和建议 252
第 5 步：启用依赖项发现（可选） 253
第 6 步：进行第一次弹性测试（可选） 253
系统、用户旅程和服务 254
概述：系统、用户旅程和服务层次结构 255
创建和管理系统 256
创建和管理用户旅程 258
创建和管理服务 260
在服务中添加和移除资源 264
从外部注册表导入应用程序上下文 266
查看服务拓扑 267
示例：对多账户应用程序进行建模 267
弹性政策 269
了解弹性策略 270
策略组件 270
创建弹性策略 271
在用户旅程和服务级别应用策略 271
策略继承和多级评估 272
管理和更新政策 273
评测 274
依赖项发现 274
失效模式评估 281
弹性测试 288
弹性测试的工作原理 288
配置测试 289
可用测试 290
测试运行和报告 300
用于弹性测试的 IAM 执行角色 301
仪表板和报告 341
中央 SRE 控制面板概述 341

Service-level 观点 341
按政策、账户、地区和系统筛选 342
生成合规性和弹性态势报告 342
AWS Organizations 集成 344
下一代 Resilience Hub 中的多账户治理概述 345
设置组织集成 346
Service-Linked 角色 347
跨账户应用弹性策略 347
查看组织范围的弹性状况 347
管理会员账号登录 347
委派管理员设置所需的 IAM 权限 348
迁移来源 AWS Resilience Hub 349
下一代 Resilience Hub 有哪些变化 350
概念映射： AWS Resilience Hub v1 到下一代弹性中心 350
Step-by-step 迁移指南 351
定价过渡 352
迁移期间的已知限制 353
安全性 353
IAM 角色和权限参考 354
数据加密 359
VPC 端点 373
CloudTrail 整合 374
合规性注意事项 374
监控 375
CloudWatch 指标参考 375
CloudTrail 事件日志 376
EventBridge 通知 378
为下一代 Resilience Hub 设置 CloudWatch 警报 385
限额和限制 386
服务配额 386
申请增加配额 387
问题排查 388
依赖关系发现问题 388
失效模式评估问题 389
IAM 和权限错误 391
AWS 组织配置问题 392

资源发现问题 393
弹性测试问题 397
已知问题和变通方法 398
API 参考 399
发出 API 请求和身份验证 399
操作 399
数据类型 406
错误代码 408
文档历史记录 409
AWS 词汇表 410
..... cdxi

AWS Resilience Hub

AWS Resilience Hub 是您管理和改善应用程序弹性状况的中心位置 AWS。 AWS Resilience Hub 使您能够定义自己的复原力目标，根据这些目标评估您的应变能力，并实施改进建议。

主题

- 什么是 AWS Resilience Hub?
- 开始使用
- 使用 AWS Resilience Hub
- 使用 AWS Resilience Hub 用于描述和管理应用程序的 API
- 中的安全性 AWS Resilience Hub
- 弹性检查 AWS 务
- 使用其他服务
- 的文档历史记录 AWS Resilience Hub 用户指南

什么是 AWS Resilience Hub?

AWS Resilience Hub 是您管理和改善应用程序弹性状况的中心位置 AWS。 AWS Resilience Hub 使您能够定义自己的复原力目标，根据这些目标评估您的应变能力，并根据 AWS Well-Architected 框架实施改进建议。在内部 AWS Resilience Hub，你还可以创建和运行 AWS Fault Injection Service 实验，模仿现实生活中对应用程序的干扰，以帮助你更好地了解依赖关系并发现潜在的弱点。 AWS Resilience Hub 提供持续增强应变能力所需的所有 AWS 服务和工具的中心位置。 AWS Resilience Hub 与其他服务配合使用以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 AWS 弹性服务和参考资料

AWS 弹性服务	文档链接
AWS 弹性灾难恢复	弹性灾难恢复
AWS Backup	什么是 AWS Backup

AWS 弹性服务	文档链接
亚马逊应用程序恢复控制器 (ARC) (ARC)	什么是亚马逊应用程序恢复控制器 (ARC)

主题

- AWS Resilience Hub — 弹性管理
- AWS Resilience Hub — 弹性测试
- AWS Resilience Hub 概念
- AWS Resilience Hub 表象人格
- AWS Resilience Hub 支持的资源
- AWS Resilience Hub 和 “我的应用程序”

AWS Resilience Hub — 弹性管理

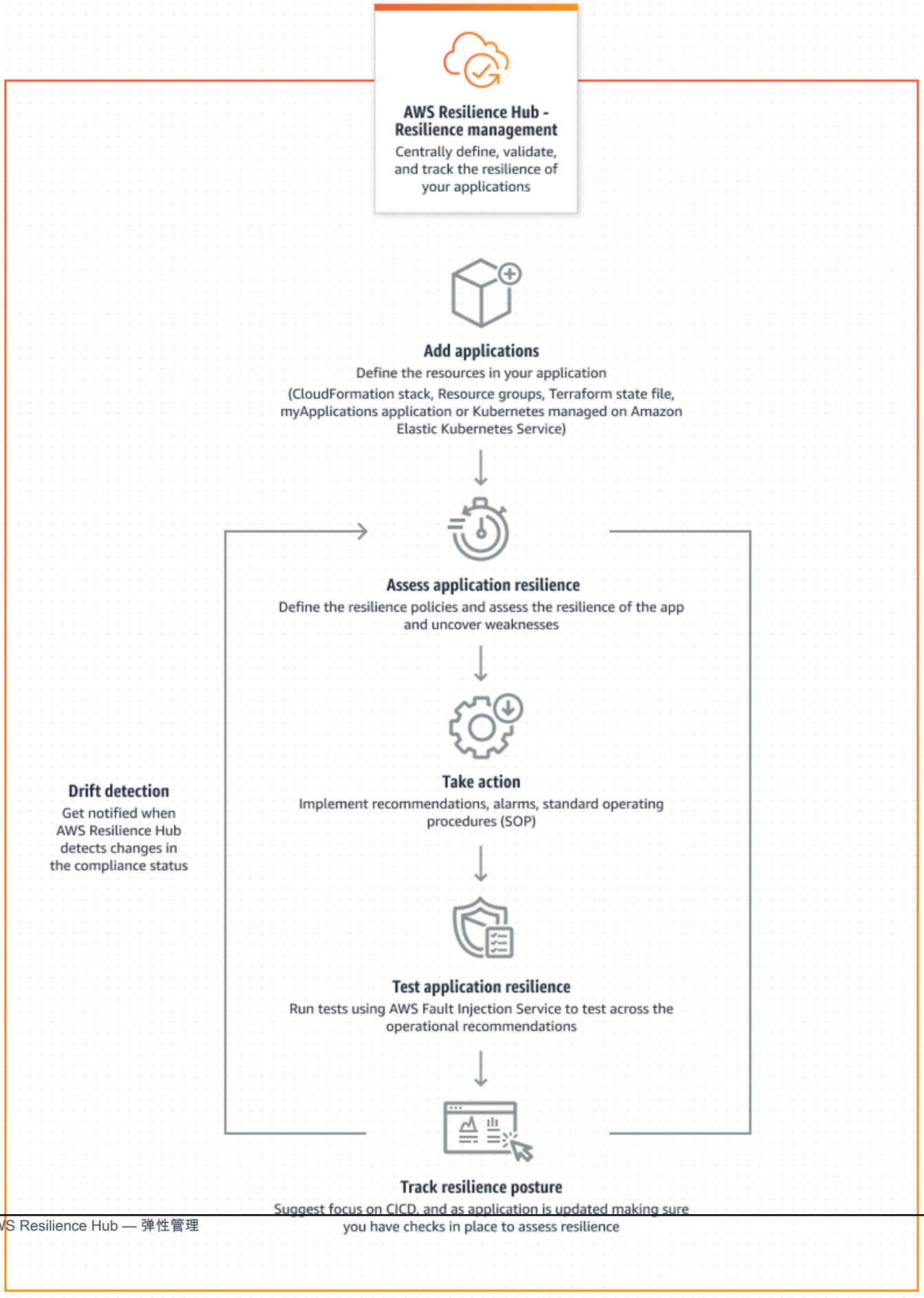
AWS Resilience Hub 为您提供定义、验证和跟踪 AWS 应用程序弹性的中心位置。 AWS Resilience Hub 帮助您保护应用程序免受中断，降低恢复成本以优化业务连续性，从而帮助满足合规性和法规要求。你可以用它 AWS Resilience Hub 来执行以下操作：

- 分析您的基础架构并获取建议，以提高应用程序的弹性。除了提高应用程序弹性的架构指导外，这些建议还为满足您的弹性政策、实施测试、警报和标准操作程序 (SOP) 提供了代码，您可以在集成和交付 (CI/CD) 管道中部署和运行应用程序。
- 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，您可以将其 AWS Resilience Hub 添加到 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。

操作方法 AWS Resilience Hub 方式

下图概述了 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, myApplications 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、亚马逊弹性 Kubernetes 服务集群中导入资源来描述您的应用程序 AWS Resource Groups，或者您可以从 MyApplications 中已定义的应用程序中进行选择。

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 AWS Well-Architected 框架中的最佳实践来分析应用程序的组成部分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。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 来继续跟踪应用程序的弹性状况。如果发生停机，操作员可以在中查看停机情况 AWS Resilience Hub 并启动相关的恢复过程。

AWS Resilience Hub — 弹性测试

AWS Resilience Hub 支持增强与 AWS FIS. 的集成。这种集成 AWS Resilience Hub 允许根据所评估应用程序的特定环境使用 AWS FIS 操作和场景提供量身定制的建议。运行推荐的实验或使用该 AWS FIS 服务进行自己的测试将直接有助于提高应用程序的弹性分数。

这些 AWS FIS 操作和场景通过创建中断事件来测试应用程序的弹性状况，以便您可以观察应用程序的响应情况。 AWS FIS 提供多个预建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，请完成一the section called “先决条件”节中定义的先决条件。 AWS FIS

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

AWS FIS 导航菜单选项和参考资料

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 库
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，以及指向包含从 AWS Resilience Hub 控制台开始使用 AWS FIS 测试的过程的相关 AWS FIS 文档的链接。

AWS FIS 下拉菜单选项和参考资料

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理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 应用程序是一组 AWS 受支持的资源，这些资源经过持续监控和评估，以管理其弹性状况。

应用程序组件

一组作为一个 AWS 整体运行和失败的相关资源。例如，如果您有主数据库和副本数据库，则这两个数据库属于同一个应用程序组件 (AppComponent)。

AWS Resilience Hub 确定哪些 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 报告您的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 RTO 和 RPO 目标为 24 小时。 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。其中一项或多项 AppComponents 不符合政策目标。例如，您为跨 AWS 区域的中断选择了 RTO 和 RPO 目标为 24 小时，但您的数据库配置不包括任何跨区域恢复方法，例如全局复制和备份副本。

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。

偏差检测

AWS Resilience Hub 在对应用程序运行评估时运行偏移通知，以检查 AppComponent 配置更改是否影响了应用程序的合规性状态。此外，它还检查和检测诸如在应用程序输入源中添加或删除资源之类的更改，并发出相应的通知。为了进行比较， AWS Resilience Hub 使用先前的评估，其中应用程序组件符合策略。 AWS Resilience Hub 检测以下类型的漂移：

- 应用程序策略偏差 — 此偏差类型可识别所有在先前评估中符合政策但在当前评估中未遵守的政策。AppComponents
- 应用程序资源漂移 -此漂移类型标识当前应用程序版本中的所有漂移资源。

弹性评测

AWS Resilience Hub 使用漏洞和潜在补救措施清单来衡量选定策略在灾难中恢复和继续工作的有效性。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 生成的分数表明您的应用程序在满足应用程序弹性政策、警报、标准操作程序 (SOP) 和测试方面的建议的程度如何。

中断类型

AWS Resilience Hub 帮助您评估针对以下类型中断的弹性：

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。

AWS FIS 实验

AWS Resilience Hub 建议使用 AWS FIS 操作进行实验，以验证应用程序对抗不同类型中断的能力。这些中断包括应用程序、基础架构、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 建议一组标准操作程序，并建议在中断之前准备、测试和衡量标准操作程序，以确保及时恢复。

AWS Resilience Hub 表象人格

构建企业应用程序需要不同的跨职能团队共同努力，例如基础架构、业务连续性、应用程序所有者和其他负责监控应用程序的利益相关者。来自不同团队的不同角色有助于在中构建和管理应用程序 AWS Resilience Hub，每个角色和职责不同。要了解有关向不同角色授予权限的更多信息，请参阅the section called “AWS Resilience Hub 角色和 IAM 权限参考”。

要开始在中创建应用程序和运行评估 AWS Resilience Hub，我们建议您创建以下角色：

- 基础架构应用程序管理器 -具有此角色的用户负责设置、配置和维护基础架构和应用程序资源，确保应用程序的可靠性和安全性。他们的职责包括以下内容：
  - 确保定期部署和更新应用程序
  - 监控系统性能
  - 排查问题
  - 实施备份和灾难恢复计划
- 业务连续性经理 — 具有此角色的用户负责制定应用程序策略和确定应用程序的业务关键性。他们的职责包括以下内容：
  - 在制定政策时做出关键决定
  - 评估业务关键性
  - 为关键应用程序分配资源
  - 评估和管理风险
- 应用程序所有者 -具有此角色的用户有责任确保应用程序的高可用性和可靠性。他们的职责包括以下内容：
  - 定义关键性能标识符以衡量和监控应用程序性能并确定瓶颈
  - 为多个利益相关者组织培训
  - 确保以下文档是最新的：
    - 应用程序架构
    - 部署流程
    - 监控配置
    - 性能优化技术
- Read-only 访问权限 -具有此角色的用户仅限于只读权限。他们的职责包括通过监控弹性分数、运营建议和弹性建议来保持应用程序性能和运行状况的可见性并进行监督。此外，他们还负责确定问题、趋势和需要改进的领域，以确保应用程序满足组织的目标。

AWS Resilience Hub 支持的资源

在发生中断时影响应用程序性能的资源完全由 AWS Resilience Hub 顶级资源（例如`AWS::RDS::DBInstance`和）支持`AWS::RDS::DBCluster`。

要详细了解在评估中 AWS Resilience Hub 加入来自所有支持服务的资源所需的权限，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

AWS Resilience Hub 支持来自以下 AWS 服务的资源：

- 计算
  - Amazon Elastic Compute Cloud（Amazon EC2）

    > **Note**
    >
    > AWS Resilience Hub 不支持使用旧的亚马逊资源名称 (ARN) 格式访问亚马逊 EC2 资源。新的 ARN 格式使用您的 AWS 账户 ID，增强了在集群中标记资源的能力，还可以跟踪集群中运行的服务和任务的成本。
    >
    > - 旧格式（已弃用）— `arn:aws:ec2:<region>::instance/<instance-id>`
    > - 新格式 — `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`
    >
    > 有关新 ARN 格式的更多信息，请参阅将您的 Amazon ECS 部署迁移到新的 ARN 和资源 ID 格式。

  - 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
  - 亚马逊 ElastiCache
- 联网和内容分发
  - Amazon Route 53
  - Elastic Load Balancing
  - 网络地址转换（NAT）
- 仓储服务
  - Amazon Elastic Block Store （Amazon EBS)
  - Amazon Elastic File System (Amazon EFS)
  - Amazon Simple Storage Service（Amazon S3）
  - 适用于 Windows File Server 的 Amazon FSx
- 其他
  - Amazon API Gateway

- 亚马逊应用程序恢复控制器 (ARC)（亚马逊 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的实例，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，在评估过程中发现资源实例， 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 支持亚马逊 EKS 和亚马逊 ECS AWS Fargate。
> - AWS Resilience Hub 支持将 AWS Backup 资源评估作为以下服务的一部分：
>   - Amazon EBS
>   - Amazon EFS
>   - Amazon S3
>   - Amazon Aurora Global Database
>   - Amazon DynamoDB
>   - Amazon RDS 数据服务
>   - 适用于 Windows File Server 的 Amazon FSx
> - 亚马逊 ARC 仅 AWS Resilience Hub 评估全球 Amazon DynamoDB、弹性负载均衡、亚马逊 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 在应用程序组件中对资源进行分组。
> - 目前， AWS Resilience Hub 如果亚马逊 EKS 集群位于或应用程序是在启用 AWS 选择加入的区域中创建的，则不支持对 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）
  - 当前，仅 AWS Resilience Hub 支持以下 ElastiCache 资源引擎类型：
    - Redis OSS 引擎

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。
- Non-top 级别资源 — 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
>
> - 您无法使用 AWS Resource Groups（亚马逊 Route 53 RecordSets 和 API-GW HTTP）和亚马逊 Aurora Global 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 MyApplications 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
> - 在将应用程序的资源导入到的过程中 AWS Resilience Hub，某些资源可能会被忽略。当资源被忽略时，这意味着它们根本无法导入。但是，标记为不支持的资源目前与不兼容，AWS Resilience Hub 但将来可能会受到支持，因此可以将其包含在评估应用程序中。此外，如果某些资源不受支持，则 AWS Resilience Hub 可能会忽略这些资源 AWS Resource Groups。有关支持的资源的更多信息 AWS Resource Groups，请参阅可与之配合使用的资源类型 AWS Resource Groups 和标签编辑器。

AWS Resilience Hub 和 “我的应用程序”

MyApplications 仪表板中的弹性控件简化了评估和监控应用程序弹性的过程。它使您能够快速评估在 myApplications 中定义的应用程序的弹性，而无需在控制台中手动重新创建它们。 AWS Resilience Hub 这种集成方法将 MyApplications 的应用程序管理功能与的弹性评估功能相结合 AWS Resilience Hub，使您能够利用这两个平台的优势。通过整合应用程序定义和弹性评估功能，Resiliency 控件简化了工作流程，使您能够从集中位置访问相关信息并采取行动增强弹性。通过 “弹性” 控件评估应用程序时，将 AWS Resilience Hub 执行以下操作：

- 在中创建所选应用程序 AWS Resilience Hub。
- 自动发现和映射与模型相关的资源。
- 创建并分配新的韧性策略，其中包含恢复时间目标（RTO）和恢复点目标（RPO）的预定义值。对于 RTO 来说是四个小时，对于 RPO 来说是一小时。生成评估后，您可以修改弹性策略或从 AWS Resilience Hub 控制台分配不同的策略。有关更新弹性策略和附加其他策略的更多信息，请参阅。管理弹性策略
- 评估应用程序对弹性策略中定义的 RTO 和 RPO 的弹性，以确定应用程序架构需要改进的领域。故障情景包括可用区故障、区域中断和其他潜在中断。
- 在初始评估后持续监控应用程序的资源和配置更改，如果任何更改影响应用程序的弹性，则发出警报或更新。

> **Note**
>
> 在开始评估之前，我们建议您使用以下方法评估进行评估所涉及的潜在成本 AWS Resilience Hub。有关详细的定价信息，请参阅定AWS Resilience Hub 价。

在评估您的应用程序后，您可以通过选择 Go to AWS Resilience Hub 来访问插件的 AWS Resilience Hub 全部功能，在 AWS Resilience Hub 控制台中查看应用程序的详细信息。将应用程序从 MyApplications 添加到的过程 AWS Resilience Hub 受以下规则和约束条件的约束：

- 您只能将一个 MyApplications 应用程序关联到中的一个应用程序。 AWS Resilience Hub也就是说，您可以通过在 MyApplications 控制面板中通过 R esiliency 控件运行评估，或者在控制台中描述应用程序时完成该使用 “我的应用程序” 应用程序程序，将 MyApplications 应用程序关联到应用程序。 AWS Resilience Hub AWS Resilience Hub

- 您只能包含、评估和查看与 MyApplications 环境位于相同 AWS 区域和 AWS 账户边界内的 MyApplications 应用程序。在不同 AWS 区域或不同 AWS 账户下创建的应用程序将无法通过此插件显示或访问。
- 您只能在 MyApplications 仪表板中添加、移除和更新资源。当您从 MyApplications 仪表板修改应用程序资源时，必须重新导入 AWS Resilience Hub 才能查看中的资源更改。 AWS Resilience Hub

了解详情

有关在 MyApplications 仪表板中管理应用程序和资源的更多信息，请参阅 AWS Console Home 文档中的以下主题：

- 我的应用程序开启了 AWS什么？
- 在 myApplications 中创建您的第一个应用程序
- 管理资源
- 弹性小工具

有关在中描述应用程序和运行评估的更多信息 AWS Resilience Hub，请参阅以下主题：

- 对现有设备进行弹性评估 myApplications 申请来自 弹性 第一次使用小部件
- 重新运行现有弹性评估 myApplications 申请来自 弹性 小部件
- 查看 “弹性” 小工具中的评估摘要

开始使用

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

主题

- 先决条件
- 将应用程序添加到 AWS Resilience Hub

先决条件

在使用之前 AWS Resilience Hub，必须满足以下先决条件：

- AWS 帐户-为您要在其中使用的每种账户类型（primary/secondary/资源帐户）创建一个或多个 AWS 帐户。 AWS Resilience Hub有关创建和管理 AWS 账户的更多信息，请参阅以下内容：
  - 首次 AWS 使用用户 — 入门：您是首次 AWS 使用用户吗？
  - 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，则必须设置一个新角色并为配置必要的 IAM 权限， AWS Resilience Hub 才能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 “操作方法 AWS 弹性中心可与 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、群组和角色添加 IAM 权限，您可以使用我们的 AWS 托管策略 (the section called “AWS 托管策略”)。与自己编写策略相比，使用 AWS 托管策略来涵盖您的常见用例要容易 AWS 账户 得多。 AWS Resilience Hub 为 AWS 托管策略添加额外权限，以扩展对其他 AWS 服务的支持并添加新功能。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 “在中进行弹性评估 AWS Resilience Hub”
  - 如果您未使用 AWS 托管策略向用户、群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和保护 AWS 应用程序免受中断影响：

- 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。您可以从现有的 MyApplications 应用程序、 AWS CloudFormation 堆栈中收集资源 AWS Resource Groups ，或者制定适当的弹性策略。描述应用程序

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

- 开始添加应用程序
- 选择如何管理此应用程序
- 添加资源集合
- 设置 RTO 和 RPO
- 设置预定评测和偏移通知
- 设置权限
- 配置应用程序配置参数
- 添加标签
- 查看并发布您的 AWS Resilience Hub 应用程序
- 对你进行评估 AWS Resilience Hub 应用程序

开始添加应用程序

首先， AWS Resilience Hub 描述 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。

在中描述您的应用程序的详细信息 AWS Resilience Hub

本节向您介绍如何在中描述现有 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

选择如何管理此应用程序

选择如何管理此应用程序

除了 AWS CloudFormation 堆栈 AWS Resource Groups、MyApplications应用程序和Terraform状态文件外，您还可以添加位于亚马逊弹性Kubernetes服务（亚马逊 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、MyApplications 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 AWS CloudFormation 堆栈、 AWS Resource Groups Terraform 状态文件和 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

添加资源集合

添加资源集合

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：

- 添加资源集合
- 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 “我的应用程序” 应用程序
- 使用 Terraform 状态文件

使用 AWS CloudFormation 堆栈

选择包含您要在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堆栈，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 堆栈来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。

   要使用位于不同或不同区域的堆栈 AWS 账户，请选择在区域外添加堆栈旁边的右箭头，在输入堆栈 ARN 框中输入堆栈的亚马逊资源名称 (ARN)，然后选择添加堆栈 ARN。 AWS 有关 ARN 的更多信息，请参阅《AWS 一般参考》中的 Amazon 资源名称（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、不同区域或同时使用这两个区域的资源，请选择资源组 ARN: 旁边的右箭头，在 “输入资源组 ARN” 框 AWS Resource Groups 中输入的亚马逊资源名称 (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 资源名称（ARN）。

使用 “我的应用程序” 应用程序

选择要包含在其中的 MyApplications 应用程序 AWS Resilience Hub

将 MyApplications 应用程序包含在 AWS Resilience Hub

1. 选择 “我的应用程序”。
2. 从 “选择应用程序” 下拉列表中选择一个应用程序。

使用 Terraform 状态文件

选择包含您要在描述的应用程序中使用的 Amazon 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. 在选择状态文件:: 部分中，选择浏览 S3 以导航到您的 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 URI 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 “在 S3 中选择档案” 对话框中，从 “存储桶” 部分选择您的 Amazon 简单存储服务存储桶。
4. 从对象部分中，选择一个密钥，然后选择选择。

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 “允许 AWS Resilience Hub 访问您的 Amazon EKS 集群”

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集群，也可以来自不同的账户或不同的区域。 AWS 账户

> **Note**
>
> AWS Resilience Hub 要评估您的亚马逊 EKS 集群，您必须在 EKS 集群和命名空间部分手动向每个 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. 在 1. 选择 EKS 集群部分，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. 要使用位于不同或不同 AWS 账户区域的亚马逊 EKS 集群，请选择在其他账户或地区内添加 EKS 集群旁边的右箭头，在输入 EKS ARN 框中输入亚马逊 EKS 集群的亚马逊资源名称 (ARN)，然后选择添加 EKS ARN。 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 “允许 AWS Resilience Hub 访问您的 Amazon EKS 集群”。

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 AWS Resilience Hub 是否包含所选 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

设置 RTO 和 RPO

设置 RTO 和 RPO

您可以根据自己的 RTO/RPO 目标定义新的弹性策略，也可以选择具有预定义 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。

定义自己的 RTO/RPO 目标

1. 选择 “创建新的弹性策略” 选项。
2. 在 “输入策略名称” 框中（在 “名称” 下）中输入弹性策略的名称。

   我们已经使用自动生成的名称预先填充了此字段。您可以选择使用相同的名称，也可以选择不同的名称。
3. （可选）在描述框中输入弹性策略的描述。
4. RTO/RPO 在RTO/RPO 目标部分定义你的。

> **Note**
>
> - 我们已经为您的应用程序预先填充了默认 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，在评估您的申请时，尽可能低的评估结果接近于零。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. 要定义 RTO/RPO 基础架构和可用区，请选择右箭头展开基础架构 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 R TO 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想要定义区域 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 “设置预定评估和偏差通知”

设置预定评测和偏移通知

AWS Resilience Hub 允许您设置预定评估和偏差通知，以便每天评估您的应用程序，并在检测到偏差时收到通知。

设置漂移通知

1. 要每天评估您的应用程序，请打开 “每日自动评估” 。

   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 `AWSResilienceHubAsssessmentExecutionPolicy`

     角色，使用 the section called “操作方法 AWS 弹性中心可与 IAM 配合使用” 中的相应过程。

2. 要在 AWS Resilience Hub 检测到任何偏离弹性策略的情况或其资源出现偏差时收到通知，请打开“应用程序偏离时获得通知”。

   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**
   >
   > - 要启用 AWS Resilience Hub 向您的 Amazon SNS 主题发布通知，必须使用适当的权限配置您的 Amazon SNS 主题。有关配置用户权限的信息，请参阅 the section called “允许 AWS Resilience Hub 向您的 Amazon SNS 主题发布内容”。
   > - 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。

   要使用位于不同地区 AWS 账户 或不同区域的亚马逊 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

设置权限

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. 要选择将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 角色的亚马逊资源名称 (ARN)，则 AWS Resilience Hub 将使用您在选择 IAM 角色下拉列表中为所有账户选择的 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 IAM 控制台中创建 AWS Resilience Hub 角色中的程序。
- 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，具体取决于哪种账户类型（主账户或辅助账户）。

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，某些 AWS Resilience Hub 功能（例如偏移通知）可能无法按预期运行，并且您为创建新应用程序提供的输入将被忽略。

下一步

配置应用程序配置参数

配置应用程序配置参数

本部分允许您使用 AWS 弹性灾难恢复提供跨区域故障转移支持的详细信息。 AWS Resilience Hub 将使用此信息提供弹性建议。

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，我们已使用您的账户 ID 预先填充了此字段 AWS Resilience Hub，该编号可以更改。
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

添加标签

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 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

查看并发布您的 AWS Resilience Hub 应用程序

查看并发布您的 AWS Resilience Hub 应用程序

创建应用程序后，您仍然可以查看该应用程序并编辑其资源。完成后，选择发布以发布应用程序。

> **Note**
>
> AWS Resilience Hub 在后台扫描您的应用程序资源，检查是否可以以更有效的方式对它们进行分组，从而提高评估的准确性。如果 AWS Resilience Hub 确定了可以分组为相关资源 AppComponents，则会在应用程序页面的应用程序结构选项卡中显示资源分组建议信息警报，您可以通过选择查看建议来查看这些资源。有关更多信息，请参阅 the section called “AWS Resilience Hub 资源分组建议”。

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

对你进行评估 AWS Resilience Hub 应用程序

对你进行评估 AWS Resilience Hub 应用程序

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，您可以在其中运行弹性评估。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 帮助您提高应用程序的弹性， AWS 并缩短应用程序中断时的恢复时间。

主题：

- AWS Resilience Hub 摘要
- AWS Resilience Hub 仪表板
- 描述和管理 AWS Resilience Hub 应用程序
- 管理弹性策略
- 在中运行和管理弹性评估 AWS Resilience Hub
- 通过弹性小工具运行和管理弹性评估
- 管理警报

- 管理标准操作程序
- 管理 AWS Fault Injection Service 实验
- 了解弹性分数
- 将操作建议集成到您的应用程序中 CloudFormation

AWS Resilience Hub 摘要

AWS Resilience Hub 提供了带有图表和图形的可视化摘要，使您可以 at-a-glance查看应用程序在多个 AWS 服务和资源中的弹性状况。这份全面而简洁的直观摘要使您能够快速识别潜在的弹性差距，确定操作的优先顺序，并跟踪增强应用程序从中断中恢复能力方面的进展。当您选择导出时，如果您是首次导出指标，则会在您访问的区域中 AWS Resilience Hub 创建一个新的 Amazon S3 存储桶 AWS Resilience Hub。此 Amazon S3 存储桶仅为首次创建，成功完成后将用于保存导出的指标。在 Amazon S3 中存储导出的数据需要支付额外费用。有关这些费用的更多信息，请参阅 Amazon S3 定价。

小组件中的图表和图形可帮助您理解以下内容：

- 应用程序的总体弹性分数和当前运行状态概述。
- 突出显示不符合既定策略或偏离推荐配置的应用程序，从而可能违反策略或偏离最佳实践。此外，它还会突出显示特定领域，使您能够确定优先顺序并解决这些问题。
- 需要立即关注的关键资源或应用程序。
- 关于加强弹性实践的建议，例如实施警报、进行 AWS Fault Injection Service (AWS FIS) 实验和制定标准操作程序。这些建议会随着时间的推移进行跟踪，使您可以监控实施进度并衡量对应用程序整体弹性状况的影响。

小组件

- 应用程序状态
- 按资源类型划分的热门基础架构建议
- 基础设施建议
- 未执行的业务建议
- 警报推荐
- SOP 建议
- AWS FIS 实验建议

- 有漂移的应用程序
- 弹性得分
- 弹性评分排名前 10 的应用程序
- 按策略划分的应用程序状态

应用程序状态

此控件可显示您的应用程序是否符合弹性策略。在弹出窗口中选择应用程序计数旁边的数字，即可在“应用程序” 窗格中查看所有关联的应用程序。要查看您创建的所有应用程序，请选择查看应用程序。有关在中管理应用程序的更多信息 AWS Resilience Hub，请参阅查看 AWS Resilience Hub 应用程序摘要。

按资源类型划分的热门基础架构建议

此小组件显示上次成功评估中针对您的 AWS 每种资源类型提供的基础设施建议数量，以改善其弹性状况。您可以通过将鼠标悬停在详细信息上方或导航到详细信息来识别详细信息。要查看您创建的所有应用程序，请选择查看应用程序。有关基础设施建议的更多信息，请参阅查看弹性建议。

基础设施建议

此小组件列出了最多 10 个应用程序，这些应用程序的基础设施建议数量达到上次成功评估中为改善其弹性状况而提供的最大数量。要查看您创建的所有应用程序，请选择查看应用程序。有关基础设施建议的更多信息，请参阅查看弹性建议。

您可以使用以下方法识别详细信息：

- 应用程序名称-您在中定义应用程序时提供的应用程序的名称 AWS Resilience Hub。
- 计数 — 表示上次成功评估 AWS Resilience Hub 中提供的基础架构建议数量。选择数字即可查看评估报告中提供的所有基础架构建议。
- 上次评估-表示上次成功评估您的申请的日期和时间。

未执行的业务建议

此小组件列出了最多 10 个应用程序，这些应用程序在上次成功评估中提供了最大数量的未实施操作建议，以改善其弹性状况。要查看您创建的所有应用程序，请选择查看应用程序。有关操作建议的更多信息，请参阅审查操作建议。

您可以使用以下方法识别详细信息：

- 应用程序名称-您在中定义应用程序时提供的应用程序的名称 AWS Resilience Hub。
- 计数-表示上次成功评估 AWS Resilience Hub 中提供的操作建议数量。选择数字即可查看评估报告中所有未执行的操作建议。
- 上次评估时间-表示上次成功评估您的申请的日期和时间。

警报推荐

此小组件列出了为在选定时间段内改善弹性状况而提供的所有 Amazon CloudWatch 警报建议。不同的类别（“已实施”、“未实现” 和 “已排除”）表示它们在您的应用程序中的实现状态。您可以通过将鼠标悬停在每个类别的Amazon CloudWatch 警报推荐上方或导航到它们来查看这些建议的数量。要查看您创建的所有应用程序，请选择查看应用程序。有关警报建议的更多信息，请参阅审查操作建议。

SOP 建议

此小组件列出了为在选定时间段内改善弹性状况而提供的所有标准操作程序 (SOP) 建议。不同的类别（“已实施”、“未实现” 和 “已排除”）表示它们在您的应用程序中的实现状态。您可以通过将鼠标悬停在每个类别的 SOP 建议上方或导航到它们来查看这些建议的数量。要查看您创建的所有应用程序，请选择查看应用程序。有关操作建议的更多信息，请参阅审查操作建议。

AWS FIS 实验建议

此控件列出了为在选定时间段内改善弹性姿势而提供的所有 AWS FIS 实验建议。不同的类别（“已实施”、“未实施”、“部分实施” 和 “已排除”）表示它们在您的应用程序中的实现状态。您可以通过将鼠标悬停在每个类别的 AWS FIS 实验推荐上方或导航到它们来查看这些建议的数量。要查看您创建的所有应用程序，请选择查看应用程序。有关 AWS FIS 实验建议的更多信息，请参阅管理标准操作程序。

有漂移的应用程序

此小组件列出了所有在上次成功评估中偏离先前合规状态的应用程序。要查看您创建的所有应用程序，请选择查看应用程序。有关在中管理应用程序的更多信息 AWS Resilience Hub，请参阅查看 AWS Resilience Hub 应用程序摘要。

您可以使用以下方法识别详细信息：

- 应用程序名称-您在中定义应用程序时提供的应用程序的名称 AWS Resilience Hub。
- 政策偏差 — 选择应用程序名称旁边的数字，以查看在上一次评估中符合策略但在当前评估中未遵守政策的所有应用程序组件。

- 资源漂移 — 选择下面的数字，查看最新导入中与其配置相比的所有资源。

弹性得分

此小组件显示选定时间段内最多五个应用程序的应用程序弹性分数趋势。您可以查看应用程序的弹性分数，方法是将鼠标悬停在与应用程序名称关联的行上，或者导航到该行，然后选择应用程序名称以查看应用程序摘要。要查看您创建的所有应用程序，请选择查看应用程序。有关弹性分数的更多信息，请参阅了解弹性分数。

弹性评分排名前 10 的应用程序

此控件列出了最近评估中弹性得分最低的 10 个应用程序，重点介绍了需要立即关注以提高其弹性的应用程序。要查看您创建的所有应用程序，请选择查看应用程序。有关弹性分数的更多信息，请参阅了解弹性分数。

您可以使用以下方法识别详细信息：

- 应用程序名称-您在中定义应用程序时提供的应用程序的名称 AWS Resilience Hub。
- 弹性分数-运行评估后由 AWS Resilience Hub 您的应用程序确定的总体弹性分数。
- 上次评估时间-表示上次成功评估您的申请的日期和时间。

按策略划分的应用程序状态

此小组件列出了您的所有政策，以及已违反、符合或尚未根据这些政策进行评估的应用程序数量。要查看您创建的所有策略，请选择查看策略。有关弹性分数的更多信息，请参阅管理弹性策略。

您可以使用以下方法识别详细信息：

- 策略名称-表示您在中定义策略时提供的策略名称 AWS Resilience Hub。
- 类型-表示附加到应用程序的策略（弹性策略）的类型。
- 策略名称-表示违反弹性策略中定义的 RTO 和 RPO 目标的应用程序数量。
- 满足的应用程序-表示符合弹性策略的应用程序数量。
- 未评估的应用程序-表示尚未根据弹性策略进行评估的应用程序数量。
- 弹性分数-运行评估后由 AWS Resilience Hub 您的应用程序确定的总体弹性分数。
- 上次评估时间-表示上次成功评估您的申请的日期和时间。

AWS Resilience Hub 仪表板

仪表板提供了应用程序组合弹性状态的全面视图。仪表板汇总和组织弹性事件（例如，数据库不可用或弹性验证失败）、警报以及来自 CloudWatch 和 AWS Fault Injection Service (AWS FIS) 等服务的见解。

仪表板还会为每个经过评估的应用程序生成弹性分数。该分数表示在根据推荐的弹性策略、警报、恢复标准操作程序 (SOPs) 和测试进行评估时，您的应用程序的性能如何。您可以使用此分数来衡量随时间推移而提高的韧性。

要查看 AWS Resilience Hub 仪表板，请从导航菜单中选择 “控制面板”。“控制面板” 页面显示以下部分：

应用程序状态

应用程序状态表明是否已评估应用程序是否符合其所附的弹性政策。此外，评估完成后，状态还会显示您的应用程序的输入源是否已被修改。在以下每种状态下选择一个数字，即可在 “应用程序” 页面中查看所有具有相同状态的应用程序：

- 策略中的应用程序-表示所有符合其所附弹性策略的应用程序。
- 违反策略的应用程序-表示所有不符合其所附弹性策略的应用程序。
- 未评估的应用程序-表示尚未评估或跟踪其合规性的所有应用程序。
- 应用程序漂移 — 表示所有已偏离其弹性策略或其资源是否已转移的应用程序。

随着时间的推移应用程序弹性得分

通过随时间推移的应用程序弹性分数，您可以查看过去 30 天内应用程序的弹性图表。虽然下拉菜单可以列出 10 个应用程序，但一次 AWS Resilience Hub 只能显示最多四个应用程序的图表。有关弹性分数的更多信息，请参阅了解弹性分数。

> **Note**
>
> AWS Resilience Hub 不会同时运行预定评估。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 “查看指标” CloudWatch，在控制面板中创建和查看有关应用程序弹性的更精细信息。 CloudWatch 有关更多信息 CloudWatch，请参阅 Amazon CloudWatch 用户指南中的使用控制面板。

已实现警报

本部分列出了您在 Amazon 中为监控所有应用程序 CloudWatch 而设置的所有警报。有关更多信息，请参阅 查看警报。

已实施的实验

本节列出了您在所有应用程序中实现的所有故障注入实验。有关更多信息，请参阅 查看 AWS FIS 实验。

描述和管理 AWS Resilience Hub 应用程序

AWS Resilience Hub 应用程序是一组 AWS 资源，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，您需要提供应用程序名称、来自一个或多个 CloudFormation 堆栈的资源以及相应的弹性策略。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，必须发布该应用程序，以便对其进行弹性评估。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。

要查看应用程序页面，请从导航窗格中选择应用程序。您可以通过以下方式在 “应用程序” 页面中识别您的应用程序：

- 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。
- 合规状态 — AWS Resilience Hub 将应用程序状态设置为 “已评估” 、“未评估” 、“违反政策” 或 “已检测到更改”。
  - 已评估 - AWS Resilience Hub 已评估您的申请。
  - 未评估 - AWS Resilience Hub 尚未评估您的申请。
  - 违反了政策 - 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) 的目标。在重新评估您的应用程序的灵活性 AWS Resilience Hub 之前，请查看并使用提供的建议。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 已检测到对与您的应用程序相关的弹性策略所做的更改。您必须重新评估您的应用程序 AWS Resilience Hub ，以确定您的应用程序是否符合灵活性政策的目标。

- 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 -这表示您的应用程序不是每天自动评估的 AWS Resilience Hub ，您必须手动评估您的应用程序。
- 偏移状态 - 指示您的应用程序是否偏离了上一次成功的评测，并设置以下状态之一：
  - 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。此外，它还表明是否添加或移除了当前应用程序版本中包含的输入源中的资源。
  - 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。此外，它还表明未添加或移除当前应用程序版本中包含的输入源中的资源。
- 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**
>
> AWS Resilience Hub 只有当您使用 Amazon ECR 作为镜像存储库时，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。

以下主题显示了描述 AWS Resilience Hub 应用程序的不同方法以及如何管理它们。

主题

- 查看 AWS Resilience Hub 应用程序摘要
- 编辑 AWS Resilience Hub 应用程序资源
- 管理应用程序组件
- 发布新的 AWS Resilience Hub 应用程序版本
- 查看所有 AWS Resilience Hub 应用程序版本
- 查看的资源 AWS Resilience Hub 应用程序
- 正在删除 AWS Resilience Hub 应用程序
- 应用程序配置参数

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. 从导航窗格中选择 “应用程序”。
2. 在应用程序页面上，选择要查看的应用程序的名称。

应用程序摘要页面包含以下部分。

主题

- 评估摘要
- 摘要
- 应用程序弹性
- 已实施的警报
- 已实施的实验

评估摘要

本节概述了上次成功的评估，并重点介绍了作为可操作见解的关键建议。 AWS Resilience Hub 使用 Amazon Bedrock 生成式 AI 功能来帮助用户将注意力集中在由 AWS Resilience Hub提供的最关键的弹性建议上。通过关注关键项目，您可以专注于提高应用程序弹性状况的最关键建议。选择一项建议以查看其摘要，然后选择查看详细信息以在评估报告的相关部分中查看有关建议的更多详细信息。有关审阅评估报告的更多信息，请参阅the section called “查看评估报告”。

> **Note**
>
> - 此评估摘要仅在美国东部（弗吉尼亚北部）地区提供。
> - 由 Amazon Bedrock 上的大型语言模型 (LLMs) 生成的评估摘要只是建议。当前的生成式人工智能技术水平并不完美，也不是万无一失 LLMs 的。偏见和错误答案虽然很少见，但应该预料到。在使用法学硕士的输出之前，请先查看评估摘要中的每项建议。

摘要

本节在以下各节中提供了所选应用程序的摘要：

- 应用程序信息-本节提供有关所选应用程序的以下信息：
  - 应用程序状态-表示应用程序的状态。
  - 描述-应用程序的描述。
  - 版本-表示应用程序当前评估的版本。
  - 弹性策略-表示附加到应用程序的弹性策略。有关弹性策略的更多信息，请参阅 管理弹性策略。
- 应用程序漂移 — 本节重点介绍在对所选应用程序进行评估以检查其是否符合其弹性策略时检测到的偏差。此外，它还会检查自上次发布应用程序版本以来是否添加或删除了任何资源。此部分显示以下信息：
  - 政策偏差 — 选择下面的数字可查看在上一次评估中符合政策但在当前评估中未符合政策的所有应用程序组件。
  - 资源漂移 — 选择下面的数字以查看最新评估中的所有漂移资源。

应用程序弹性

弹性分数部分中显示的指标来自该应用程序的最新弹性评估。

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。该分数反映了您的应用程序对满足应用程序弹性策略、警报、标准操作程序 (SOPs) 和测试的 AWS Resilience Hub 建议的遵守程度。

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 建议使用一个警报和一个 SOP 进行一次测试。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。

已实施的警报

应用程序摘要已实施警报部分列出了您在 Amazon 中 CloudWatch 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 管理 AWS Fault Injection Service 实验。

编辑 AWS Resilience Hub 应用程序资源

要获得准确而有用的弹性评估，请确保更新您的应用程序描述并与您的实际 AWS 应用程序和资源相匹配。评测报告、验证和建议均基于列出的资源。如果您在 AWS 应用程序中添加或移除资源，则应在中反映这些更改 AWS Resilience Hub。

AWS Resilience Hub 提供有关应用程序来源的透明度。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。资源分组为逻辑应用程序组件 (AppComponents)。您可以编辑 AppComponents 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）版本来添加或更新您的应用程序资源。 AWS Resilience Hub 使用应用程序的发布版本（包括更新的资源）来运行弹性评估。

评测应用程序的弹性

1. 在导航窗格中，选择 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. 选择查看选项卡以查看您的应用程序的评测报告。

启用预设评估

1. 在导航窗格中，选择 应用程序。
2. 在应用程序页面上，选择要为其启用预设评估的应用程序。
3. 打开 “每天自动评估”。

禁用预设评估

1. 在导航窗格中，选择 应用程序。
2. 在应用程序页面上，选择要为其启用预设评估的应用程序。
3. 关闭 “每天自动评估”。

> **Note**
>
> 禁用预定评估将禁用偏差通知。

4. 选择关闭。

为您的应用程序启用漂移通知

1. 在导航窗格中，选择 应用程序。
2. 在应用程序页面上，选择要为其启用偏差通知或编辑漂移通知设置的应用程序。
3. 您可以通过选择以下选项之一来编辑漂移通知：

   - 从 “操作” 中选择 “启用偏移通知”。

- 在 “应用程序漂移” 部分中选择 “启用通知”。

4. 完成中的步骤设置预定评测和偏移通知，然后返回此过程。
5. 请选择启用。

   启用漂移通知也将启用预定评估。

编辑应用程序的偏移通知

> **Note**
>
> 如果您启用了计划评估（开启了每日自动评估）和偏差通知，则此程序适用。

1. 在导航窗格中，选择 应用程序。
2. 在应用程序页面上，选择要为其启用偏差通知或编辑漂移通知设置的应用程序。
3. 您可以通过选择以下选项之一来编辑漂移通知：

   - 在操作中，选择编辑偏移通知。
   - 在 “应用程序漂移” 部分中选择 “编辑通知”。

4. 完成中的步骤设置预定评测和偏移通知，然后返回此过程。
5. 选择保存。

更新应用程序的安全权限

1. 在导航窗格中，选择 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 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 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 附加。

编辑输入源、资源和应用程序 AppComponents 的输入源

1. 在导航窗格中，选择 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. 要编辑输入源、资源和应用程序 AppComponents 的输入源，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，如果您选择从 AWS CloudFormation 堆栈导入的源名称，您将被重定向到 AWS CloudFormation 控制台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、MyApplications 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 “向您的 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，我们根据多个搜索条件对资源 AWS Resilience Hub 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 是用于识别 AWS CloudFormation 堆栈、Terraform 状态文件、手动添加的应用程序、MyApplications 应用程序或中的资源的名称。 AWS Resource Groups

> **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`声明一个 Amazon EC2 实例。有关对 AppComponent 资源进行分组的更多信息，请参阅在应用程序组件中对资源进行分组。

- 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，如果您选择从 AWS CloudFormation 堆栈导入的源名称，则系统会将您重定向到上的堆栈详细信息页面 AWS CloudFormation。
- 源类型 - 输入源的类型。输入源包括 AWS CloudFormation 堆栈、MyApplications 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 — 为该资源实际分配的标识符，例如 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。
- 帐户-拥有物理资源的 AWS 帐户。

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 添加资源集合 中的相应步骤，然后返回到此过程。

   c. 选择保存。

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. AppComponent 从下AppComponent拉列表中选择一个。

   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 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. 选择保存。

9. 要更改 AppComponent，请选择资源， AppComponent从 “操作” 中选择 “更改”，然后完成以下步骤：

   a. AppComponent 从下AppComponent拉列表中选择一个。

   b. 选择 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。

编辑您的应用程序的 AppComponents

1. 要编辑您的应用程序，请选择该AppComponents选项卡。 AppComponents

> **Note**
>
> 有关对 AppComponent 资源进行分组的更多信息，请参阅在应用程序组件中对资源进行分组。

该AppComponents部分列出了资源归入的所有逻辑组件。您可以 AppComponents 通过以下方式识别：

- AppComponent nam e — 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 t ype — 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 “新建”， AppComponent然后完成以下步骤：

   a. 在名称框 AppComponent 中输入的AppComponent名称。作为参考，我们在此字段中预先填充了示例名称。

   b. 从 “类型” 下拉列表中选择AppComponent类型。 AppComponent

   c. 选择保存。

3. 要编辑 AppComponent，请选择一个 AppComponent，然后 AppComponent从 “操作” 中选择 “编辑”。

4. 要删除 AppComponent，请选择一个 AppComponent，然后选择 AppComponent从操作中删除。

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 发布新的 AWS Resilience Hub 应用程序版本。

管理应用程序组件

应用程序组件 (AppComponent) 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，则这两个数据库属于同一个数据库 AppComponent。AWS Resilience Hub 有管理哪些 AWS 资源可以属于哪 AppComponent 种类型的规则。例如，`DBInstance`可以属于`AWS::ResilienceHub::DatabaseAppComponent`而不是`AWS::ResilienceHub::ComputeAppComponent`。

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::ElastiCache::CacheCluster
  - AWS::ElastiCache::GlobalReplicationGroup
  - AWS::ElastiCache::ReplicationGroup
  - AWS::ElastiCache::ServerlessCache
  - 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 Amazon FSx for Windows 文件服务器。

  - AWS::S3::Bucket

主题

- 在应用程序组件中对资源进行分组

在应用程序组件中对资源进行分组

将应用程序及其资源导入 AWS Resilience Hub 时，在导入应用程序 AppComponent 时 AWS Resilience Hub 会尽最大努力将相关资源分组为相同的资源，但是分组可能并不总是百分之百准确。由于这些服务具有严格的依赖关系，需要特定的分组配置，因此某些资源会被阻止进行手动分组，因此在适用时会自动进行分组。有关被阻止进行手动分组的服务的完整列表，请参阅the section called “已屏蔽用于手动分组的服务”。

AWS Resilience Hub 成功导入应用程序及其资源后，将执行以下活动：

- 扫描您的资源以检查是否可以将其重新分组为新资源 AppComponents以提高评估的准确性。
- 如果 AWS Resilience Hub 确定了可以重新分组为新资源的资源 AppComponents，则它会显示与推荐相同的资源，并允许您接受或拒绝相同的资源。在中 AWS Resilience Hub，分配给分组建议的置信度表示应根据资源的属性和元数据对资源进行分组的确定程度。高置信度表示 AWS Resilience Hub 置信度为 90% 或以上，表示该组中的资源是相关的，应组合在一起。中等置信度表示 AWS Resilience Hub 置信度介于 70% 和 90% 之间，表示该组中的资源是相关的，应组合在一起。

> **Note**
>
> AWS Resilience Hub 需要正确的分组，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。

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。
- 将运行相同应用程序的 Amazon EC2 实例分组到一个实例下 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。

有关通过查看和包括资源分组建议的更多信息 AWS Resilience Hub，请参阅以下主题：

- AWS Resilience Hub 资源分组建议

- 手动将资源分组为 AppComponent

已屏蔽用于手动分组的服务

AWS Resilience Hub 阻止您手动对某些 AWS 服务的资源进行分组，以防止出现可能影响应用程序弹性评估和建议的配置错误。这些服务会根据其依赖关系和配置自动分组。当您定义包含这些资源的应用程序时 AWS Resilience Hub，它会分析它们的关系、依赖关系和弹性要求，以创建最佳分组，从而确保准确的评估结果。

因手动分组而被屏蔽的 AWS 服务列表：

- Amazon API Gateway
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic File System
- Amazon Relational Database Service
- Amazon S3
- Amazon Simple Queue Service
- FSx 适用于 Windows 文件服务器
- NAT 网关

AWS Resilience Hub 资源分组建议

本节介绍如何在中生成和查看资源分组建议 AWS Resilience Hub。

> **Note**
>
> 您可以使用`AWSResilienceHubAsssessmentExecutionPolicy` AWS 托管策略授予使用所需的必要 IAM 权限。 AWS Resilience Hub 有关 AWS 托管策略的更多信息，请参阅AWSResilienceHubAsssessmentExecutionPolicy。

查看资源分组建议

1. 在导航窗格中，选择 应用程序。

2. 选择添加应用程序页面，选择要查看其资源分组建议的应用程序名称。
3. 选择应用程序结构选项卡。
4. 如果 AWS Resilience Hub 显示信息提醒，请选择查看建议以查看所有资源分组建议。否则，请完成以下步骤以手动生成资源分组建议：

   a. 选择资源。
   b. 从 “操作” 菜单中选择 “获取分组建议”。

      AWS Resilience Hub 扫描您的资源，以检查如何以最佳方式将其分组为相关资源 AppComponents ，从而提高评估的准确性。如果 AWS Resilience Hub 得知您的资源可以分组在一起，则会显示相同资源的信息提醒。
   c. 如果显示信息警报，请选择查看建议以查看所有资源分组建议。

   您可以使用以下方法 AppComponents 在 “查看资源分组建议” 部分中标识：

   - AppComponent 名称-将在其中 AppComponent 对资源进行分组的名称。
   - 置信度 — 表示分组建议中 AWS Resilience Hub 的置信度。
   - 资源计数-表示将在中分组的资源数量 AppComponent。
   - AppComponent t ype — 表示的类型 AppComponent。

查看将要分组的资源 AppComponents

1. 完成查看资源分组建议过程中的步骤，然后返回到此过程。
2. 在 “查看资源分组建议” 部分，选中复选框（AppComponent 名称旁边）以查看将在选定资源内分组的所有资源 AppComponent。如果选中多个复选框，则 AWS Resilience Hub 会显示动态生成的已选推荐部分，该部分将所选建议 AppComponents 按各自的 AppComponent类型进行分组。选择每 AppComponent 种类型下方的数字，以查看将在所选类型中组合在一起的所有资源 AppComponent。

   您可以使用以下方法确定将在 “资源” 部分所选资源 AppComponent 中进行分组的资源：

   - 逻辑 ID - 指示资源的逻辑 ID。逻辑 ID 是用于识别 AWS CloudFormation 堆栈、Terraform 状态文件、MyApplications 应用程序或中的资源的名称。 AWS Resource Groups
   - 物理 ID — 为资源分配的实际标识符，例如 Amazon EC2 实例 ID 或 Amazon S3 存储桶名称。
   - 类型-表示资源的类型。
   - AWS 区域-资源所在的区域。

接受资源分组建议

1. 完成查看资源分组建议过程中的步骤，然后返回到此过程。
2. 在 “查看资源分组建议” 部分，选中AppComponent名称旁边的所有复选框。要查找特定的AppComponent，请在 “查找 AppComponents” 框中输入 AppComponent名称。

   > **Note**
   >
   > 默认情况下， AWS Resilience Hub 显示所有资源分组建议。要使用以前拒绝的资源分组建议筛选表格，请从 “查找” AppComponents 框旁边的下拉菜单中选择 “以前已拒绝”。

3. 选择 Accept (接受)。
4. 在 “接受资源分组建议” 对话框中选择 “接受”。

   AWS Resilience Hub 如果资源分组成功，则会显示信息警报。如果您只接受了资源分组建议的子集，则查看资源分组建议部分会显示您尚未接受的所有资源分组建议。

拒绝资源分组建议

1. 完成查看资源分组建议过程中的步骤，然后返回到此过程。
2. 在 “查看资源分组建议” 部分，选中AppComponent名称旁边的所有复选框。要查找特定的AppComponent，请在 “查找 AppComponents” 框中输入 AppComponent名称。

   > **Note**
   >
   > 默认情况下， AWS Resilience Hub 显示所有资源分组建议。要使用以前拒绝的资源分组建议筛选表格，请从 “查找” AppComponents 框旁边的下拉菜单中选择 “以前已拒绝”。

3. 选择 Reject (拒绝)。
4. 选择拒绝资源分组建议的原因之一，然后在 “拒绝资源分组建议” 对话框中选择 “拒绝”。

   AWS Resilience Hub 显示确认相同内容的信息警报。如果您只拒绝了资源分组建议的子集，则查看资源分组建议部分会显示您尚未接受的所有资源分组建议。

手动将资源分组为 AppComponent

本节介绍如何手动将资源分组到中， AppComponent 并 AppComponent 向中的资源分配不同的资源 AWS Resilience Hub。

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. 选中 “逻辑 ID” 旁边的复选框以选择要分组的所有资源。

> **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。
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。

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. 选中逻辑 ID 旁边的复选框以选择资源。
7. AppComponent从 “操作” 菜单中选择 “更改”。
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。

发布新的 AWS Resilience Hub 应用程序版本

按照中所述对 AWS Resilience Hub 应用程序资源进行更改后编辑 AWS Resilience Hub 应用程序资源，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 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 새 버전 발행。
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，或者您可以使用建议的默认名称 AWS Resilience Hub。
6. 选择发布。

   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 在中运行和管理弹性评估 AWS Resilience Hub。

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 显示应用程序自创建之日起的先前版本 AWS Resilience Hub。

查看应用程序的所有版本

1. 在导航窗格中，选择 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，请在 “查看所有版本” 前选择加号 (+) 。 AWS Resilience Hub 分别使用草稿和当前发布状态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。

查看的资源 AWS Resilience Hub 应用程序

查看应用程序资源

1. 在导航窗格中，选择 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 是用于识别 AWS CloudFormation 堆栈、Terraform 状态文件、MyApplications 应用程序或中的资源的名称。 AWS Resource Groups

> **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，请参阅在应用程序组件中对资源进行分组。
- 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，如果您选择从 AWS CloudFormation 堆栈导入的源名称，您将被重定向到上的堆栈详细信息页面 AWS CloudFormation。
- 源类型 — 输入源的类型。
- AppComponent type — 输入源的类型。输入源包括 AWS CloudFormation 堆栈、MyApplications 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— 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。
- 帐户 -拥有物理资源的 AWS 账户。

4. 选择保存并更新。

正在删除 AWS Resilience Hub 应用程序

在达到 50 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 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。

应用程序配置参数章节列出了对 AWS 弹性灾难恢复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，故障转移配置。
- 目的-指明 AWS Resilience Hub 要求提供信息的原因。
- 参数-表示特定于应用领域的详细信息，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，此参数仅使用一个故障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配置参数 AWS 弹性灾难恢复 并发布应用程序，以包含更新的弹性评估参数。

更新应用程序配置参数

1. 在导航窗格中，选择 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。弹性策略包含的信息和目标，您可以使用这些信息和目标来评估您的应用程序是否有望从中断类型（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 R TO 和 RPO 字段中输入零值。但是，在评估您的申请时，尽可能低的评估结果接近于零。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。在流程结束时， AWS Resilience Hub 评估您的应用程序如何根据弹性策略中的恢复目标进行衡量。

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推荐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。这些级别包括：基础IT核心服务、关键任务、关键、重要和 Non-critical。

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

在中 AWS Resilience Hub，您可以创建弹性策略。弹性策略包含的信息和目标，您可以使用这些信息和目标来评估应用程序能否从中断类型（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。当您进行评估时，AWS Resilience Hub 确定对应用程序的估算是否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。在流程结束时， AWS Resilience Hub 评估您的应用程序如何根据弹性策略中的目标进行衡量。

> **Note**
>
> 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，在评估您的申请时，尽可能低的评估结果接近于零。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 “为您的应用程序添加标签 ”，从 the section called “开始添加应用程序” 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。

   Turn-on 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。

   Turn-on 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：

   - Non-critical 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。

在中运行和管理弹性评估 AWS Resilience Hub

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。您还可以测试在您指定的条件下 SOPs 工作效果如何。

主题：

- 在中进行弹性评估 AWS Resilience Hub
- 查看评估报告
- 删除弹性评估

在中进行弹性评估 AWS Resilience Hub

您可以从中的 AWS Resilience Hub多个位置进行弹性评估。有关应用程序的更多信息，请参阅 the section called “管理 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” 部分选择评估报告。

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 SOPs和测试的建议
- 如何创建和管理标签以搜索和筛选 AWS 资源

评测报告

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。

检测到的资源漂移

本部分列出了在最新版本的已发布应用程序中之后添加或删除的所有资源。选择 “重新导入输入源”，在 “输入源” 选项卡中重新导入所有输入源（其中包含漂移的资源）。选择 “发布并评估”，将更新的资源包含在应用程序中，并获得准确的弹性评估。

您可以使用以下方法识别偏移的输入源：

- 逻辑 ID - 指示资源的逻辑 ID。逻辑 ID 是用于识别 AWS CloudFormation 堆栈、Terraform 状态文件、MyApplications 应用程序或中的资源的名称。 AWS Resource Groups
- 更改-表示输入资源是添加还是移除。
- 源名称 - 指示资源名称。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，如果您选择从 AWS CloudFormation 堆栈导入的源名称，则系统会将您重定向到上的堆栈详细信息页面 AWS CloudFormation。
- 资源类型 - 指示资源类型。
- 帐户-表示拥有物理资源的 AWS 帐户。
- 区域 - 指示资源所在的 AWS 区域。

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定区域 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 AWS Fault Injection Service）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，则可能是因为在的限制范围内 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

操作建议包含设置警报和通过 AWS CloudFormation 模板 AWS FIS 进行实验的建议。 SOPs

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 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 Amazon 简单存储服务 URI，而不是 CLI/API 使用本地文件作为输入。

在中 AWS Resilience Hub，您可以执行以下操作：

- 您可以配置选定的警报 SOPs、和 AWS FIS 实验。要配置警报和 AWS FIS 实验，请选择相应的建议并输入一个唯一的名称。 SOPs 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推荐的选定警报和 AWS FIS 实验。 SOPs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 SOPs，用于包含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 “在中进行弹性评估 AWS Resilience Hub” 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 Amazon 或任何其他第三方服务提供商等 AWS 服务中实现了这些警报 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。

在应用程序中加入或排除推荐的标准操作程序 (SOPs)

1. 要排除推荐项 SOPs，请完成以下步骤：
   a. 在 “标准操作程序” 选项卡下，从SOPs表中选择所有要排除的 SOPs （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. 从 “操作” 中选择 “排除选定项”，将所选内容 SOPs 从应用程序中排除。
   c. 从 “排除推荐” 对话框中，选择以下原因之一（可选），然后选择 “排除选定项”，将所选内容 SOPs 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 SOPs 中实现了这些功能，请选择此选项。
- 不相关 — 如果 SOPs 不适合您的业务需求，请选择此选项。
- 实施起来太复杂 — 如果您认为实施起来太复杂 SOPs ，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 SOPs，请完成以下步骤：

   a. 在 “标准操作程序” 选项卡下，从SOPs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 “包括推荐” 对话框中，选择 “包括选定内容”，将所有选定内容包括在应用程序 SOPs 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。

通过弹性小工具运行和管理弹性评估

AWS Resilience Hub 使您能够对在 MyApplications in Resilency 控件中创建和管理的应用程序进行评估。无论何时对应用程序进行修改，都建议通过弹性控件或控制台运行弹性评估。 AWS Resilience Hub 在此评估期间，将根据既定策略和最佳实践对每个应用程序组件的配置进行评估。根据该评估，评估为设置警报、制定标准操作程序 (SOP) 和实施测试策略提供建议。实施这些配置建议可以提高恢复程序的速度和效率，确保更快的事件响应并最大限度地减少潜在的停机时间。

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。

主题：

- 通过弹性小工具进行弹性评估
- 查看 “弹性” 小工具中的评估摘要

通过弹性小工具进行弹性评估

对于在 MyApplications 控件中创建的应用程序，您现在可以通过弹性控件和控制台运行弹性评估。AWS Resilience Hub 有关从 AWS Resilience Hub 控制台运行弹性评估的更多信息，请参阅在中进行弹性评估 AWS Resilience Hub。

对现有设备进行弹性评估 myApplications 申请来自 弹性 第一次使用小部件

1. 登录 AWS 管理控制台。
2. 展开左侧边栏并选择 myApplications。
3. 选择要为其运行评估的应用程序。

   作为先决条件，请确保您在 AWS 控制台中添加了 “弹性” 控件。要添加此小部件，请完成以下步骤。

   a. 在 Console Home 仪表板的右上角或右下方，选择 +添加控件。
   b. 选择拖动指示器（由控件标题栏左上角的六个垂直点表示），然后将其拖动到您的 Console Home 仪表板。
4. 选择 “评估应用程序” 。
5. 要选择将用于访问当前账户中资源的现有 IAM 角色，请选择使用 IAM 角色，然后从选择 IAM 角色下拉列表中选择一个 IAM 角色。

   如果您想使用当前 IAM 用户来发现您的应用程序资源，请选择使用当前 IAM 用户权限，然后 AWS Resilience Hub在 “使用当前 IAM 用户发现应用程序资源” 部分中选择我知道我必须手动配置权限才能启用所需功能。
6. 选择 “评估” 。

   或者，启用 “每日自动评估” AWS Resilience Hub 以允许每天评估您的应用程序，而无需支付任何额外费用。

   AWS Resilience Hub 执行以下操作：

   - 在中创建应用程序 AWS Resilience Hub 并自动发现和映射关联资源。
   - 创建并分配新的韧性策略，其中包含恢复时间目标（RTO）和恢复点目标（RPO）的预定义值。也就是说，RTO 为四小时，RPO 为一小时。生成评估后，您可以修改弹性策略或从 AWS Resilience Hub 控制台分配不同的策略。有关更新韧性策略和附加其它策略的更多信息，请参阅管理韧性策略。
   - 评测应用程序对于 RTO 和 RPO 的韧性，并持续监控资源和配置更改以及发布结果。

> **Note**
>
> 在开始评测之前，建议使用 AWS Resilience Hub来评估进行评测所涉及的潜在成本。有关详细的定价信息，请参阅定AWS Resilience Hub 价。

重新运行现有弹性评估 myApplications 申请来自 弹性 小部件

1. 登录 AWS 管理控制台。
2. 展开左侧边栏并选择 myApplications。
3. 选择要重新评估的应用程序。

   作为先决条件，请确保您在 AWS 控制台中添加了 “弹性” 控件。要添加此小部件，请完成以下步骤。

   a. 在 Console Home 仪表板的右上角或右下方，选择 +添加控件。
   b. 选择拖动指示器（由控件标题栏左上角的六个垂直点表示），然后将其拖动到您的 Console Home 仪表板。
4. 从 “弹性” 控件中选择 “重新评估”。

   或者，启用 “每日自动评估” AWS Resilience Hub 以允许每天评估您的应用程序，而无需支付任何额外费用。

查看 “弹性” 小工具中的评估摘要

R esiliency 控件显示评估结果的快照，这将为您提供有关 MyApplications 应用程序的弹性、潜在漏洞、关键性能指标 (KPI) 和建议的改进措施的最重要和最可行的见解。可以使用以下内容，从最新的评测中了解有关应用程序韧性状况的更多信息：

- 韧性得分历史 - 此图表显示应用程序的韧性得分长达一年的趋势。
- 韧性得分 - 表示最新评测中评估的应用程序的韧性得分。该分数反映了您的应用程序在满足应用程序弹性政策以及实施警报、标准操作程序 (SOP) 和 () 实验方面的建议的程度如何。 AWS Fault Injection Service AWS FIS选择该数字可在 AWS Resilience Hub 控制台摘要选项卡下的 “弹性分数” 部分中查看更多信息。有关更多信息，请参阅 评测报告。
- 策略违规情况 -选择以下数字，在 AWS Resilience Hub 控制台的 “评估报告” 窗格中查看违反应用程序所附策略的所有应用程序组件 (AppComponents)。有关更多信息，请参阅 评测报告。

- 政策偏差 - AppComponents 表示在上一次评估中遵守了政策但在当前评估中未遵守政策的人。选择以下数字， AppComponents 在 AWS Resilience Hub 控制台的 “评估报告” 窗格中查看。有关更多信息，请参阅 评测报告。
- 资源偏差 -选择以下数字，在控制台的 “评估报告” 窗格中查看从最新评估中转移出的所有资源。AWS Resilience Hub 有关更多信息，请参阅 评测报告。
- 前往 Resilience Hub — 选择此选项可在 AWS Resilience Hub 控制台中打开应用程序。

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有正确的 Amazon CloudWatch 警报。

此外， AWS Resilience Hub 现在可以自动检测任何已配置的 Amazon CloudWatch 警报并将其集成到其弹性评估中，从而更全面地了解应用程序的弹性状况。这项新功能将 AWS Resilience Hub 建议与您当前的监控设置相结合，简化了警报管理并提高了评估的准确性。如果您已实施了 Amazon CloudWatch 警报 AWS Resilience Hub 但未自动检测到该警报，则可以排除该警报，并将原因选择为 “已实施”。有关排除建议的更多信息，请参阅包含或排除操作建议。

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
- 查看警报

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 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 CloudFormation 控制台创建堆栈。

要根据 AWS Resilience Hub 建议创建警报，您必须为推荐的警报创建 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 “在中进行弹性评估 AWS Resilience Hub” 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)。
- 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。

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 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。

要将 AWS Resilience Hub 建议包括在内，请输入您的代码库

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 “警报” 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 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 访问该 CloudFormation 模板，也可以将其下载并放入您的代码管道或通过 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。在已实现的警报表中，您可以使用以下信息识别已实施的警报：

- 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。

查看应用程序中实现的警报

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)。
   - 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。

管理标准操作程序

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。提前做好准备、测试和测量，以确保 SOPs 在出现运营中断时及时恢复。

根据您的应用程序组件， AWS Resilience Hub 建议 SOPs 您应准备的组件。 AWS Resilience Hub 与 Systems Manager 合作， SOPs 通过提供许多 SSM 文档来自动执行您的步骤，您可以将其用作这些 SOPs文档的基础。

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，指示在磁盘不足的情况下要运行哪个 SSM 自动化文档，以及需要哪个 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 还提供了一个名为 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 以 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 CloudFormation 模板是一个良好的开端。使用 CloudFormation 模板生成 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，您也将部署最多的 up-to-date SOP。

主题

- 根据 AWS Resilience Hub 建议制定 SOP
- 删除自定义 SSM 文档
- 使用自定义 SSM 文档而不是默认的 SSM 文档
- 正在测试 SOPs
- 查看标准操作流程

根据 AWS Resilience Hub 建议制定 SOP

要根据 AWS Resilience Hub 建议构建 SOP，您需要一个附有弹性策略的 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，您必须为推荐的 CloudFormation 模板创建模板 SOPs 并将其包含在代码库中。

为 SOP 建议创建 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 “在中进行弹性评估 AWS Resilience Hub” 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。

   完成以下过程以将 SOP 建议包含在代码库中。

在你的代码库中加入 AWS Resilience Hub 这些建议

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识别应用程序中实现的： SOPs

   - 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。
   - 来源模板-提供包含 SOP 详细信息的 AWS CloudFormation 堆栈的亚马逊资源名称 (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. 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。

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

要将为您的 SOP AWS Resilience Hub 建议的 SSM 文档替换为您创建的自定义文档，请直接在代码库中工作。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，使用中建议的默认值 AWS Resilience Hub 并根据需要对其进行自定义，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。

正在测试 SOPs

如前所述，最佳做法是在您的管道中添加 AWS FIS 实验以 SOPs 定期测试您的 CI/CD 管道；这样可以确保它们在发生中断时随时可以使用。

同时测试 AWS Resilience Hub提供的和自定义 SOPs的。

查看标准操作流程

查看通过应用程序实现 SOPs 的

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 “标准操作程序摘要” 部分，“已实施的标准操作程序” 表显示了根据 SOP 建议生成的操作程序列表。 SOPs

   您可以 SOPs 通过以下方式识别您的身份：

   - 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 SOPs 中推荐的

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 “标准操作程序” 表中，您可以使用以下信息进一步了解推荐 SOPs 操作流程：

   - 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)。有关支持的更多信息 AppComponents，请参阅中对资源进行分组 AppComponent。
   - 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 AWS CloudFormation中 AWS CloudFormation 堆栈资源的逻辑标识符。

管理 AWS Fault Injection Service 实验

本节介绍如何在中管理 AWS Fault Injection Service (AWS FIS) 实验 AWS Resilience Hub。您可以进行 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。

所有实验 AWS Resilience Hub 都是使用构建的 AWS FIS ，它们执行 AWS FIS 动作。 AWS FIS 实验仅使用针对特定 AWS 服务自定义的 AWS FIS 自动化操作（例如亚马逊 EKS 操作）。有关 AWS FIS 操作的更多信息，请参阅AWS FIS 操作参考。

您可以在默认状态下使用 AWS FIS 实验，也可以根据您的要求对其进行自定义。有关通过 AWS Resilience Hub 控制台和 AWS FIS 控制台管理 AWS FIS 实验的更多信息，请参阅以下主题：

- AWS Resilience Hub 控制台
  - 查看 AWS FIS 实验
    - 查看已实施的清单 AWS FIS 来自应用程序的实验
    - 查看推荐内容 AWS FIS 评估实验
  - the section called “跑步 AWS FIS 实验”
  - the section called “AWS Fault Injection Service 实验 failures/status 检查”
- AWS FIS 控制台
  - 管理您的 AWS FIS 实验
  - 使用场 AWS FIS 景库
  - 管理 AWS FIS 实验模板

启动、创建和运行 AWS FIS 实验

AWS Resilience Hub 通过与 AWS FIS 实验整合来简化 AWS FIS 实验。它提供量身定制的建议，并允许使用映射到您的应用程序组件 (AppComponents) 的预填充模板启动 AWS FIS 实验，从而实现高效的弹性测试。

要启动 AWS FIS 根据运营建议进行实验

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 “在中进行弹性评估 AWS Resilience Hub” 中的过程，然后返回此步骤。
6. 选择操作建议选项卡。
7. 在故障注入实验之前选择右箭头。

   本节列出了 AWS Resilience Hub 为您的应用程序推荐的所有 AWS FIS 实验，以进行压力测试和提高其弹性。根据您的实现， AWS FIS 实验分为以下状态：

   - 已实施 — 表示建议的实验已 AWS Resilience Hub 在您的应用程序中实现。选择下面的数字，查看实验表中所有已实施的实验。
   - 已部分实施 -表示建议的 AWS Resilience Hub 实验已在您的应用程序中部分实现。选择下面的数字，查看实验表中所有部分实施的实验。

- 未实现 -表示建议的实验未 AWS Resilience Hub 在您的应用程序中实现。选择下面的数字，查看实验表中所有未实施的实验。
- 已排除 — 表示您的应用程序中 AWS Resilience Hub 已排除所推荐的实验。选择下面的数字，查看实验表中所有已排除的实验。有关包括和排除推荐的实验的更多信息，请参阅包括或排除操作建议。

实验表列出了所有影响应用程序韧性评分的已实施 AWS FIS 实验。您可以使用以下信息识别 AWS FIS 实验：

- 操作名称 -表示为您的应用程序推荐的 AWS FIS 操作。选择操作名称以查看AWS FIS 实验详情页面 AppComponents 上的所有推荐内容。当状态设置为不可跟踪时，表示 AWS FIS 实验是场景。选择场景名称，在 AWS FIS 控制台的场景库页面上查看其详细信息。
- 状态 — 表示 AWS FIS 实验的当前实施状态。即已实施、部分实施、未实施和已排除。

> **Note**
>
> AWS FIS scenario 是一项仅限控制台的功能，具有多个预定义的操作。因此， AWS Resilience Hub 无法对其进行跟踪，它会将 “状态” 设置为 “不可跟踪”。

- 描述 -描述 AWS FIS 操作的目标。

8. 选择要启动实验的 AWS FIS 动作。

在 AWS FIS 实验推荐部分中，您可以使用以下信息进一步了解需要实施的 AppComponents 实验：

- 名称 — 资源分组 AppComponent 所在的名称。
- 状态 -表示 AWS FIS 操作的当前实施状态。即已实施、部分实施、未实施和已排除。

> **Note**
>
> AWS FIS scenario 是一项仅限控制台的功能，具有多个预定义的操作。因此， AWS Resilience Hub 无法对其进行跟踪，它会将 “状态” 设置为 “不可跟踪”。

- 目标选择：表示当您选择启动实验时，资源将如何包含在实验中。如果 AWS Resilience Hub 无法自动确定目标资源，请将鼠标悬停在相应的目标选择字段上，以获取有关添加这些资源的指导。

- 资源 -表示分组在下的资源数量 AppComponent。选择相应数字可在资源对话框中查看这些资源。您可以使用以下方法识别资源：
  - 逻辑 ID - 指示资源的逻辑 ID。逻辑 ID 是用于识别您的 AWS CloudFormation、Terraform 状态文件、MyApplications 应用程序、 AWS Resource Groups 资源或亚马逊弹性 Kubernetes 服务集群中的资源的名称。
  - 实际 ID：表示资源的实际分配的标识符，例如 Amazon EC2 实例 ID 或 Amazon S3 存储桶名称。
  - 类型：表示资源的类型。
  - 区域：指示资源所在的 AWS 区域。

9. 选择一个， AppComponent 然后选择 “包含” 或 “排除”，分别在 AWS FIS 实验 AppComponent 中包括或排除该对象。
10. 选择 “启动实验” 。

    AWS Resilience Hub 会将您重定向到 AWS FIS 控制台中的 “指定模板详细信息” 页面，在新选项卡中将其打开。
11. 要创建实验模板，请完成使用控制台创建实验模板中的步骤。

    此外，按照使用控制台创建实验模板中的步骤在 AWS FIS 控制台的 “指定模板详细信息” 页面中输入模板详细信息并选择 “下一步” 后， AWS Resilience Hub 会自动尝试在 “操作和目标 ” 页面中映射资源类型的操作和目标。但是，要提高覆盖范围，您可以分别选择 “添加动作” 和 “添加目标” 来手动添加动作和目标，然后完成其余过程以创建实验。

运行 AWS FIS 实验

在 AWS FIS 主机中创建实验后，按照从模板https://docs.aws.amazon.com/fis/latest/userguide/start-experiment-from-template.html开始实验中的步骤在 AWS FIS 控制台中运行实验。如果你 AWS Resilience Hub 想检测你进行的最新实验 AWS FIS，你必须进行新的评估。有关运行评估的更多信息，请参阅 在中进行弹性评估 AWS Resilience Hub。

查看 AWS FIS 实验

在中 AWS Resilience Hub，查看您为衡量 AWS 资源的灵活性以及从应用程序、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。

要从仪表板查看正在进行的 AWS FIS 实验列表，请从左侧导航菜单中选择仪表板。

在 “已实施的实验” 表中，您可以使用以下信息识别 AWS FIS 实验：

- 实验 ID — AWS FIS 实验的标识符。
- 操作 — 表示与 AWS FIS 实验相关的 AWS FIS 操作。此外，如果有多个动作，它会突出显示与 AWS FIS 实验相关的 AWS FIS 动作数量。您可以通过将鼠标指针悬停在详细信息上或导航到详细信息来识别这些详细信息。
- 实验模板 ID — 用于创建 AWS FIS 实验的实验模板的 AWS FIS 标识符。

查看已实施的清单 AWS FIS 来自应用程序的实验

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. 选择错误注入实验。

   在“已实施的实验”表中，您可以使用以下信息识别应用程序中实现的 AWS FIS 实验：

   - 实验 ID — AWS FIS 实验的标识符。
   - 操作 — 表示与 AWS FIS 实验相关的 AWS FIS 操作。此外，如果有多个动作，它会突出显示与 AWS FIS 实验相关的 AWS FIS 动作数量。您可以通过将鼠标指针悬停在详细信息上或导航到详细信息来识别这些详细信息。
   - 实验模板 ID — 用于创建 AWS FIS 实验的 AWS FIS 实验模板的标识符。

查看推荐内容 AWS FIS 评估实验

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。

   在评估表中，您可以使用以下信息识别您的评估：

   - 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 — 表明您的应用程序是否偏离了附加弹性策略中定义的 RTO 和 RPO 目标，是否偏离了先前的成功评估。
- 应用程序版本 -已评估的应用程序版本。
- 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“评估”表中选择一项评估。
5. 选择操作建议。
6. 在故障注入实验之前选择右箭头。

本节列出了 AWS Resilience Hub 为您的应用程序推荐的所有 AWS FIS 实验，以进行压力测试和提高其弹性。根据您的实现， AWS FIS 实验分为以下状态：

- 已实施 — 表示建议的实验已 AWS Resilience Hub 在您的应用程序中实现。选择下面的数字，查看实验表中所有已实施的实验。
- 已部分实施 -表示建议的 AWS Resilience Hub 实验已在您的应用程序中部分实现。选择下面的数字，查看实验表中所有部分实施的实验。
- 未实现 -表示建议的实验未 AWS Resilience Hub 在您的应用程序中实现。选择下面的数字，查看实验表中所有未实施的实验。
- 已排除 — 表示您的应用程序中 AWS Resilience Hub 已排除所推荐的实验。选择下面的数字，查看实验表中所有已排除的实验。有关包括和排除推荐的实验的更多信息，请参阅包括或排除操作建议。

实验表列出了所有影响应用程序韧性评分的已实施 AWS FIS 实验。您可以使用以下信息识别 AWS FIS 实验：

- 操作名称 -表示为您的应用程序推荐的 AWS FIS 操作。当状态设置为不可跟踪时，表示 AWS FIS 实验是场景。选择场景名称，在 AWS FIS 控制台的场景库页面上查看其详细信息。
- 状态 — 表示 AWS FIS 实验的当前实施状态。即已实施、部分实施、未实施和已排除。

> **Note**
>
> AWS FIS scenario 是一项仅限控制台的功能，具有多个预定义的操作。因此， AWS Resilience Hub 无法对其进行跟踪，它会将 “状态” 设置为 “不可跟踪”。

- 描述 -描述 AWS FIS 操作的目标。

AWS Fault Injection Service 实验 failures/status 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，请参阅查看推荐内容 AWS FIS 评估实验程序。

主题

- 正在分析 AWS FIS 使用执行实验 AWS Systems Manager
- AWS FIS 测试在 Amazon Elastic Kubernetes Service 集群中运行的 Kubernetes Pod 时实验失败

正在分析 AWS FIS 使用执行实验 AWS Systems Manager

运行 AWS FIS 实验后，可以在 AWS 系统管理器中查看执行细节。

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 “执行细节” 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：

- Test/SOP 实验执行前未部署警报模板。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。
  - 补救措施：检查输入参数并按照 “分析 AWS FIS 实验执行情况” 中的说明查看已执行的步骤，然后检查各个步骤的预期输入和输出。

AWS FIS 测试在 Amazon Elastic Kubernetes Service 集群中运行的 Kubernetes Pod 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 实验的 IAM 角色或 Kubernetes 服务账户的配置不正确。
  - 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 CloudFormation 堆栈的输出）映射到 Kubernetes 用户。
- 无法启动 P AWS FIS od：已达到失败的边车容器的最大数量。这通常发生在内存不足以运行 AWS FIS sidecar 容器时。
    - 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，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 (SOPs) 和测试方面的建议的遵守程度。根据应用程序使用的资源类型， AWS Resilience Hub 推荐警报 SOPs，并针对每种中断类型进行一组测试。

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现所有推荐的警报和测试。 SOPs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多一年的趋势。 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 — 表示恢复次数（RTO/RPOs) that need to be fixed to resolve the breaches in your application's resiliency policy. Choose the value to view the RTO/RPO应用程序评估报告中的详细信息）。
     - 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。
     - SOPs— 表示需要在您的应用程序中实现的 SOPs 建议数量。选择值 SOPs 以查看应用程序评估报告中需要修复的值。
     - 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。选择值以查看应用程序评估报告中的 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。
     - SOPs 已实施 — 表示已实施的实际贡献与其对应用程序弹性分数的最大可能贡献的 SOPs 比较。选择值以 SOPs在应用程序的评估报告中查看已实施的值。

- 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 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。
    - SOPs— 表示需要实施的 SOPs 建议数量。
    - 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。
    - SOPs— 表示从您的应用程序中排除的推荐 SOPs 人数。
    - 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

- 计算中断类型的弹性分数 AppComponents 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	说明	Formula	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)`	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 CloudWatc

评分组件	说明	Formula	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。	部分公式如下： • 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。	h 警报，则亚马逊 CloudWatch 警报覆盖范围的计算方法如下： `A = (10 + 5) / 20` 即：`A = .75 or 75 points`

评分组件	说明	Formula	示例
SOP 覆盖率（S）	标准化分数（0 -100 分）基于成功实施和排除在 AWS Resilience Hub 建议 SOPs 总数中的数量。 SOPs	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` 部分公式如下： • SOPs 已配置的总数 — 表示在 AWS CloudFormation 控制台中创建和上传 AWS CloudFormation 模板时 SOPs 配置的总数。 • SOPs 推荐的总数-表示 AWS Resilience Hub 基于应用程序资源的 SOPs 推荐数量。 • 已@@ SOPs 排除的总数-表示 SOPs 您已从应用程序中排除的推荐人数。	如果您实施了 10 个，但排除 SOPs 了 20 个 AWS Resilience Hub 建议中的 5 个 SOPs，则 SOP 覆盖范围的计算方法如下： `S = (10 + 5) / 20` 即：`S = .75 or 75 points`

评分组件	说明	Formula	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：
			• 如果您设置了区域 RTO 和 RPO 目标，P则计算方法如下：
			`P = (20 + 30)/ 100`
			即：`P = .5 or 50 points`
			• 如果您尚未设置区域 RTO 和 RPO 目标，P则计算方法如下：
			`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	说明	Formula	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 APIs 获取弹性分数 AppComponents 和中断类型：

- DescribeAppAssessment获得 RSo
- ListAppComponentCompliances获取RSao和 RSA

计算中断类型的弹性分数 AppComponents 的公式

评分组件	说明	Formula	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 AppComponent 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 SOPs、警报和会议弹性策略计算得出的。	使用以下公式计算每 AppComponent 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	说明	Formula	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 SOPs、警报和会议弹性策略计算得出的 AppComponent。	每 AppComponent 人的弹性分数使用以下公式计算： 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	说明	Formula	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) 的值T, A, S, P是针对中断类型的所有推荐测试 SOPs、警报和会议弹性策略计算得出的。	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、、测试 SOPs、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将相应增加，如未定义区域时的权重列所示。

警报、测试 SOPs、策略目标的权重

获取建议	权重
Alarms	20 点数
SOPs	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
Region	10 点数	不适用

将操作建议集成到您的应用程序中 CloudFormation

在 “操作建议” 页面中选择 “创建 CloudFormation 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 实验的模板。 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 CloudFormation 模板，该模板描述了由提供的警报建议。AWS Resilience Hub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 AWS Resilience Hub 允许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 Amazon SNS topic to which alarm status changes
 are to be sent. This must be in the same Region being deployed.",
      "AllowedPattern" : "^arn:(aws|aws-cn|aws-iso|aws-iso-[a-z]{1}|aws-us-gov):sns:
([a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-[0-9]):[0-9]{12}:[A-Za-z0-9/][A-Za-
z0-9:_/+=,@.-]{1,256}$"
    }
  },
  "Resources" : {

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

```
      },
      "Metadata" : {
        "AWS::ResilienceHub::Monitoring" : {
          "recommendationId" : "dynamodb:alarm:health-read_throttle_events:2020-04-01"
        }
      }
    },

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

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

```
}
```

修改 CloudFormation 模板

要将警报、SOP 或 AWS FIS 资源集成到主应用程序中，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 格式文件提供了模板中如何描述 DynamoDB 表的基本概述。 CloudFormation 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 SOPs 和 AWS FIS 实验的 CloudFormation 模板时，您将采用相同的方法，将硬编码参考 IDs 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，您可以执行以下 CloudFormation 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 CloudFormation 需要替换资源，则动态更新警报。

> **Note**
>
> 您可以选择更高级的方法来管理应用程序资源， CloudFormation 例如嵌套堆栈或引用单独 CloudFormation 堆栈中的资源输出。（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 Terraform by HashiCorp）也可用于配置基础设施即代码 (IaC)。

使用 AWS Resilience Hub 用于描述和管理应用程序的 API

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”

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。有关用于准备应用程序的 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

要在中创建新应用程序 AWS Resilience Hub，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。

以下示例说明如何 AWS Resilience Hub 使用 `CreateResiliencyPolicy` API `newPolicy` 为您的应用程序创建。

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 来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 会发布应用程序的新版本以及更新的版本 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。

以下示例说明如何 AWS Resilience Hub 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。

以下示例说明如何 AWS Resilience Hub 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"
    }
}
```

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

要在中运行弹性评估 AWS Resilience Hub 并监控其状态，您必须使用以下 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 Amazon CloudWatch Synthetics is setup to monitor
 the application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/
latest/monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>).
 \nMake sure that the Synthetics Name passed in the alarm dimension matches the name of
 the Synthetic Canary. It Defaults to the name of the application.\n"
        },
        {
            "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
            "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
            "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when Amazon EFS
 I/O load is more than 90% for too much time",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "09f340cd-3427-4f66-8923-7f289d4a3216",
            "referenceId": "efs:alarm:mount_failure:2020-04-01",
            "name": "AWSResilienceHub-EFSMountFailureAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when volume
 failed to mount to EC2 instance",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "* Make sure Amazon EFS utils are installed(see the <a
 href=\"https://github.com/aws/efs-utils#installation\" target=\"_blank\">docs</a>).
\n* Make sure cloudwatch logs are enabled in efs-utils (see the <a href=\"https://
github.com/aws/efs-utils#step-2-enable-cloudwatch-log-feature-in-efs-utils-config-
file-etcamazonefsefs-utilsconf\" target=\"_blank\">docs</a>).\n* Make sure that
```

```
you've configured `log_group_name` in `/etc/amazon/efs/efs-utils.conf`, for example:
`log_group_name = /aws/efs/utils`.\n* Use the created `log_group_name` in the
generated alarm. Find `LogGroupName: REPLACE_ME` in the alarm and make sure the
`log_group_name` is used instead of REPLACE_ME.\n"
      },
      {
          "recommendationId": "b0f57d2a-1220-4f40-a585-6dab1e79cee2",
          "referenceId": "efs:alarm:client_connections:2020-04-01",
          "name": "AWSResilienceHub-EFSHighClientConnectionsAlarm_2020-04-01",
          "description": "An alarm by AWS Resilience Hub that reports when client
connection number deviation is over the specified threshold",
          "type": "Metric",
          "appComponentName": "storageappcomponent-rlb",
          "items": [
              {
                  "resourceId": "fs-0487f945c02f17b3e",
                  "targetAccountId": "12345678901",
                  "targetRegion": "us-west-2",
                  "alreadyImplemented": false
              }
          ]
      },
      {
          "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
          "referenceId": "rds:alarm:health-storage:2020-04-01",
          "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
          "description": "Reports when database free storage is low",
          "type": "Metric",
          "appComponentName": "databaseappcomponent-hji",
          "items": [
              {
                  "resourceId": "terraform-20220623141426115800000001",
                  "targetAccountId": "12345678901",
                  "targetRegion": "us-west-2",
                  "alreadyImplemented": false
              }
          ]
      },
      {
          "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
          "referenceId": "rds:alarm:health-connections:2020-04-01",
          "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
          "description": "Reports when database connection count is anomalous",
          "type": "Metric",
```

```
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "f169b8d4-45c1-4238-95d1-ecdd8d5153fe",
            "referenceId": "rds:alarm:health-cpu:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceOverUtilizedCpuAlarm_2020-04-01",
            "description": "Reports when database used CPU is high",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "69da8459-cbe4-4ba1-a476-80c7ebf096f0",
            "referenceId": "rds:alarm:health-memory:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowMemoryAlarm_2020-04-01",
            "description": "Reports when database free memory is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "67e7902a-f658-439e-916b-251a57b97c8a",
```

```
            "referenceId": "ecs:alarm:health-service_cpu_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighCpuUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that triggers when CPU
utilization of ECS tasks of Service exceeds the threshold",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "fb30cb91-1f09-4abd-bd2e-9e8ee8550eb0",
            "referenceId": "ecs:alarm:health-service_memory_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighMemoryUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that
indicates if the percentage of memory that is used in the service, is exceeding
specified threshold limit",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "1bd45a8e-dd58-4a8e-a628-bdbee234efed",
            "referenceId": "ecs:alarm:health-service_sample_count:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceSampleCountAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that triggers
if the count of tasks isn't equal Service Desired Count",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
```

```
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure the Container Insights on Amazon ECS is enabled:
 (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/
deploy-container-insights-ECS-cluster.html\" target=\"_blank\">docs</a>)."
        }
    ]
}
```

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
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
```

```
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 and CapacityProviders with MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Stateful Amazon ECS service with launch type Amazon
EC2 and Amazon EFS storage, deployed in multiple AZs. AWS Backup is used to backup
Amazon EFS and copy snapshots in-Region.",
                    "suggestedChanges": [
                        "Add AWS Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove Amazon EBS volume"
                    ],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "ecs:config:ec2-multi_az-efs-backups:2022-02-16"
                }
            ]
        },
        {
            "appComponentName": "databaseappcomponent-hji",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
```

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

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

```
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 76.73,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
                            "expectedRpoInSecs": 300,
                            "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
                    "suggestedChanges": [
```

```
                        "Add read replica in the same Region",
                        "Change DB instance to a supported class (db.t3.small)",
                        "Change to Aurora",
                        "Enable cluster backtracking",
                        "Enable instance backup with retention period 7"
                    ],
                    "haArchitecture": "WarmStandby",
                    "referenceId": "rds:config:aurora-backtracking"
                }
            ]
        },
        {
            "appComponentName": "storageappcomponent-rlb",
            "recommendationStatus": "BreachedUnattainable",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
```

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

```
                    "optimizationType": "BestAttainable",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                }
            ]
        }
    ]
}
```

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 使用已发布的应用程序版本（包括更新的资源）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 “将资源排除在 AppComponent”

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部署的，则 AWS Resilience Hub 允许您使用 `CreateAppVersionResource` API 将资源手动添加到应用程序中。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 键入

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 AWS 资源，它们作为一个单元起作用和失败。例如，当您的跨区域工作负载用作备用部署时。 AWS Resilience Hub 有管理哪些 AWS 资源可以属于哪种类型的

规则 AppComponent。 AWS Resilience Hub 允许您 AppComponent 使用以下资源管理 API 将资源分组为单个资源。

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

以下示例说明如何 AWS Resilience Hub 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"
    }
}
```

以下示例说明如何 AWS Resilience Hub 使用 `UpdateAppVersionResource` API 删除前面示例中创建的空白 AppComponent 内容。

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"
    }
}
```

将资源排除在 AppComponent

AWS Resilience Hub 允许您使用 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"
            }
        ]
    }
}
```

中的安全性 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组织的要求而构建的数据中心和网络架构。

安全是您 AWS 和您的共同责任。责任共担模型将这描述为云的安全性与云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云端运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。 Third-party 作为AWS 合规计划合规计划合。要了解适用于的合规计划 AWS Resilience Hub，请参阅合规计划范围内的AWS 服务（按合规性计划划分的范围内的。
- 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。以下主题向您展示如何进行配置 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 服务来监控和保护您的 AWS Resilience Hub 资源。

内容

- 中的数据保护 AWS Resilience Hub
- 的身份和访问管理 AWS Resilience Hub

- 中的基础设施安全 AWS Resilience Hub

中的数据保护 AWS Resilience Hub

AWS 责任共担模式适用于保护 AWS Resilience Hub中的数据。如本模型所述 AWS ，负责保护运行所有网络的全球基础设施 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。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，请参阅通用数据保护条例（GDPR）中心。

出于数据保护的目的，我们建议您保护 AWS 账户 证书并使用 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。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。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。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅AWS CloudTrail 用户指南中的使用跟 CloudTrail 踪。
- 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。
- 如果在 AWS 通过命令行接口或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 终端节点。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 140-3 版》https://aws.amazon.com/compliance/fips/。

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）。这包括当你使用控制台、API或软件开发工具包 AWS 服务 使用Resilience Hub或其他 AWS 工具包时。 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 URL，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 加密您的静态数据。输入的数据使用透明 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 对在服务和其他集成 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性 (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。

的身份和访问管理 AWS Resilience Hub

AWS Identity and Access Management (IAM) AWS 服务 可以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（有权限）使用 Resilenit AWS y Hub 资源。IAM AWS 服务 是您可以免费使用的。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 操作方法 AWS 弹性中心可与 IAM 配合使用
- IAM 角色和权限
- 问题排查 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
- AWS Resilience Hub 角色和 IAM 权限参考
- 将 Terraform 状态文件导入 AWS Resilience Hub
- 正在启用 AWS Resilience Hub 访问您的亚马逊 Elastic Kubernetes 服务集群
- 正在启用 AWS Resilience Hub 发布到您的亚马逊简单通知服务主题
- 限制权限以包含或排除 AWS Resilience Hub 建议

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅问题排查 AWS 弹性中心身份和访问权限）

- 服务管理员：确定用户访问权限并提交权限请求（请参阅操作方法 AWS 弹性中心可与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅Identity-based 的策略示例 AWS Resilience Hub）

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 用户身份进行身份验证 AWS 账户根用户，或者通过代入 IAM 角色进行身份验证。

您可以使用来自 AWS IAM Identity Center（IAM 身份中心）、单点登录身份验证或证书等身份源的 Google/Facebook 证书以联合身份身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 提供 SDK 和 CLI 以加密方式签署请求。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 根用户

创建时 AWS 账户，首先要使用一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

最佳做法是，要求人类用户使用与身份提供商的联合身份验证来 AWS 服务 使用临时证书进行访问。

联合身份是来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的证书进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，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

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户 AWS 使用联合身份提供商以使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

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。策略定义了与身份或资源关联时的权限。 AWS 委托人提出请求时评估这些政策。大多数策略以 JSON 文档的 AWS 形式存储在。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

Identity-based 政策

Identity-based 策略是您附加到身份（用户、群组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

Identity-based 策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

Resource-based 政策

Resource-based 策略是您附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 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。您必须在基于资源的策略中指定主体。

Resource-based 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 的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，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 ）– 指定 AWS Organizations中组织或组织单元的最大权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略（ RCP ）– 设置对账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略（ RCP ）。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。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。要了解如何在涉及多种策略类型时 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。

操作方法 AWS 弹性中心可与 IAM 配合使用

在使用 IAM 管理对 AWS 弹性中心的访问权限之前，请了解哪些 IAM 功能可用于 Resilien AWS ce Hub。

您可以与之配合使用的 IAM 功能 AWS Resilience Hub

IAM 功能	AWS 弹性中心支持
Identity-based 政策	是
Resource-based 政策	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACL	否
ABAC（策略中的标签）	部分
临时凭证	是

IAM 功能	AWS 弹性中心支持
转发访问会话（FAS）	是
服务角色	是

要详细了解 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。

Identity-based 的政策 AWS Resilience Hub

支持基于身份的策略：是

Identity-based 策略是 JSON 权限策略文档，您可以将其附加到身份，例如 IAM 用户、用户组或角色。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》中的使用客户管理型策略定义自定义 IAM 权限。

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。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。

Identity-based 的策略示例 AWS Resilience Hub

要查看 Resilience H AWS ub 基于身份的策略的示例，请参阅。Identity-based 的策略示例 AWS Resilience Hub

Resource-based 内部的政策 AWS Resilience Hub

支持基于资源的策略：否

Resource-based 策略是您附加到资源的 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 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。

要启用跨账户访问，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。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

的政策行动 AWS Resilience Hub

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问哪些内容。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。在策略中包含操作以授予执行关联操作的权限。

要查看 Resilience H AWS ub 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 Resilience H AWS ub 基于身份的策略的示例，请参阅。Identity-based 的策略示例 AWS Resilience Hub

的政策资源 AWS Resilience Hub

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问哪些内容。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。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 Resilience Hub 资源类型及其 ARN 的列表，请参阅服务授权参考中由 Res AWS ilience Hub 定义的资源。 AWS 要了解可以使用哪些操作来指定每种资源的 ARN，请参阅 Resilience Hub 定义的 AWS 操作。

要查看 Resilience H AWS ub 基于身份的策略的示例，请参阅。Identity-based 的策略示例 AWS Resilience Hub

的策略条件键 AWS Resilience Hub

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问哪些内容。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。

`Condition` 元素根据定义的条件指定语句何时执行。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。要查看所有 AWS 全局条件密钥，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Resilience 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。 AWS 要了解可以在哪些操作和资源上使用条件键，请参阅 Resilience Hub AWS 定义的操作。

要查看 Resilience H AWS ub 基于身份的策略的示例，请参阅。Identity-based 的策略示例 AWS Resilience Hub

ACL 已输入 AWS Resilience Hub

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，但它们不使用 JSON 策略文档格式。

ABAC 和 AWS Resilience Hub

支持 ABAC（策略中的标签）：部分支持

Attribute-based 访问控制 (ABAC) 是一种授权策略，它根据称为标签的属性定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略，允许在委托人的标签与资源上的标签匹配时进行操作。

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，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。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）。

使用临时证书 AWS Resilience Hub

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并在您使用联合或切换角色时自动创建。 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 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

的转发访问会话 AWS Resilience Hub

支持转发访问会话（FAS）：是

前向访问会话 (FAS) 使用调用主体的权限 AWS 服务，同时请求 AWS 服务 向下游服务发出请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

的服务角色 AWS Resilience Hub

支持服务角色：是

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。只有在 Resilience H AWS ub 提供相关指导时，才可以编辑服务角色。

Identity-based 的策略示例 AWS Resilience Hub

默认情况下，用户和角色无权创建或修改 Resilience AWS Hub 资源。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。

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 策略（控制台）。

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

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
- 清单可用 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

Identity-based 策略决定是否有人可以在您的账户中创建、访问或删除 R AWS esilition 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，请遵循以下指南和建议：

- 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权，请使用为许多常见用例授予权限的AWS 托管策略。它们可以在您的 AWS 账户. 我们建议您通过定义特定于您的用例的 AWS 客户管理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 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》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA) — 如果您的场景需要 IAM 用户或根用户 AWS 账户，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》中的使用 MFA 保护 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 中的安全最佳实践。

使用 AWS 弹性中心控制台

要访问 Res AWS ilience Hub 控制台，您必须拥有一组最低权限。这些权限必须允许您在中列出和查看有关 Resilit AWS ion 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。

您无需为仅调用 AWS CLI 或 AWS API 的用户提供最低控制台权限。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 AWS 弹性中心控制台，还要将 AWS 弹性中心*ConsoleAccess*或*ReadOnly* AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

以下策略授予用户列出和查看 AWS Resilience Hub 控制台中所有资源的权限，但无权创建、更新或删除这些资源。

JSON

```
{
     "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完成此操作的权限，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": "*"
        }
    ]
}
```

清单可用 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。

JSON

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

```
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

开始应用程序评估

以下策略向用户授予对特定 AWS Resilience Hub 应用程序启动评估的权限。

JSON

```
{
  "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。

JSON

```
{
```

```
  "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。

JSON

```
{
  "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 应用程序推荐模板的权限。

JSON

```
{
  "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。

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 -此角色在当前账户中定义和使用。 AWS Resilience Hub 将代入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：

  - Read-only 读取资源的权限（ AWS Resilience Hub 建议您使用`AWSResilienceHubAsssessmentExecutionPolicy`托管策略）。
  - 使用信任策略来代入此角色，这允许 AWS Resilience Hub 服务主体代入此角色。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 “设置权限”。

> **Note**
>
> 如果您仅提供调用者角色名称，并且您的资源位于另一个账户中，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 将使用以下 IAM 角色来访问资源：
  - `AwsResilienceHubAdminAccountRole`，在当前账户中
  - `AwsResilienceHubExecutorAccountRole`，在其他账户中

  此外，当您配置预定评估时， AWS Resilience Hub 将代入该`AwsResilienceHubPeriodicAssessmentRole`角色。但是，`AwsResilienceHubPeriodicAssessmentRole`不建议使用，因为您必须手动配置角色和权限，而且某些功能（例如漂移通知）可能无法按预期运行。

问题排查 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 AWS 常见问题。

主题

- 我无权在中执行操作 AWS Resilience Hub
- 我无权执行 iam：PassRole
- 我想允许我之外的人 AWS 账户 访问我的 AWS 弹性中心资源

我无权在中执行操作 AWS Resilience Hub

如果您收到错误提示，指明您无权执行某个操作，则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

如果您收到无权执行`iam:PassRole`操作的错误，则必须更新您的政策，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，会出现以下示例错误。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。

我想允许我之外的人 AWS 账户 访问我的 AWS 弹性中心资源

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，可以代入角色。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，请参阅操作方法 AWS 弹性中心可与 IAM 配合使用。
- 要了解如何提供对您所拥有资源的访问权限，请参阅 IAM 用户指南中的向您拥有的另一 AWS 账户个 IAM 用户提供访问权限。 AWS 账户
- 要了解如何向第三方提供对资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方 AWS 账户 拥有的提供访问权限。
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）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访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

AWS Resilience Hub 访问权限参考

您可以使用 AWS Identity and Access Management (IAM) 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”（IAM 角色），或使用当前 IAM 用户权限（以及一组用于跨账户和计划评估的预定义角色）。在此角色中，您可以附加一个策略，该策略定义 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已添加到 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（secondary/resource账户）中，则必须在包含应用程序资源的每个账户中设置一个新角色。

> **Note**
>
> 如果您为工作负载资源定义 VPC 终端节点，请确保 VPC 终端节点策略为访问资源提供只读访问权限。 AWS Resilience Hub 有关更多信息，请参阅使用端点策略控制对 VPC 端点的访问。

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 secondary/resources 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 “用于跨账户访问的不同 AWS 账户中的角色”

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 负责访问 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 为了正确地代入您的调用者角色，该角色的信任策略必须将 AWS Resilience Hub 服务主体（res iliencehub.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（控制台）创建角色。

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。

JSON

```
{
  "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，您必须在当前 IAM user/role 中拥有调用者角色的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。以下示例显示如何向 AWS Resilience Hub 服务授予委托人权限以代入您的角色。

> **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。要向角色添加权限，请使用将策略附加到角色命令，您可以开始添加 `AWSResilienceHubAsssessmentExecutionPolicy` 托管式策略。有关托管策略的更多信息，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

示例 **`trust-policy.json`**

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

示例 **attach-policy-to-role**

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

不同角色的角色 AWS 跨账户访问账户-可选

当您的资源位于 secondary/resource 账户中时，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 secondary/resource 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 secondary/resource 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，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 secondary/resource 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。

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。要向角色添加权限，请使用将策略附加到角色命令，您可以先添加 `AWSResilienceHubAsssessmentExecutionPolicy` 托管式策略。有关托管策略的更多信息，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

示例 **`trust-policy.json`**

示例 **`create-role`**

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

示例输出

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`。

启用 AWS Resilience Hub 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 帐户。此外，您必须为预定评估的角色添加相关的信任策略 (`AwsResilienceHubPeriodicAssessmentRole`)，该策略允许该 AWS Resilience Hub 服务承担预定评估的角色。

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

   JSON

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

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Cross-account 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。
- Secondary/Resource 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 “允许 AWS Resilience Hub 访问您的 Amazon EKS 集群”。

主账户设置

您必须在主账户`AwsResilienceHubAdminAccountRole`中创建一个新角色并启用代 AWS Resilience Hub 入权限。此角色将用于访问您的 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 user/role 必须拥有代入此角色的`iam:assumeRole`权限。

- 替换 `secondary_account_id_1/2/...` 为相关的辅助账户标识符。

以下政策为您的角色提供执行者访问您 AWS 账户中其他角色的资源的权限：

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

Secondary/Resource 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：

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、群组和角色分配权限。

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使用案例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主体身份（用户、组和角色）。 AWS 当新的 AWS 托管策略启动或新 AWS 服务 的 API 操作可用于现有服务时，最有可能更新托管策略。

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，此策略向执行评估的其他 AWS 服务授予访问权限。

权限详细信息

此政策为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 模板提供了足够的权限。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：

- 亚马逊 CloudWatch (CloudWatch) — 获取您在亚马逊中设置的所有已实施警报 CloudWatch ，以监控应用程序。此外，我们还`cloudwatch:PutMetricData`用于发布`ResilienceHub`命名空间中应用程序弹性分数的 CloudWatch 指标。
- 亚马逊数据生命周期管理器-获取与您的 AWS 账户关联的亚马逊数据生命周期管理器资源并提供`Describe`权限。
- Amazon DevOps Guru — 列出与您的 AWS 账户关联的 Amazon DevOps Guru 资源并为其提供`Describe`权限。
- 亚马逊 DocumentDB — 列出与您的 AWS 账户关联的 Amazon DocumentDB 资源并为其提供`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。
- 亚马逊 ElastiCache (ElastiCache) — 为与您的 AWS 账户关联的 ElastiCache 资源提供`Describe`权限。
- 亚马逊 ElastiCache （Redis OSS）无服务器（ElastiCache （Redis OSS）无服务器）— 为与您的账户关联的 ElastiCache （Redis OSS）无服务器配置提供`Describe`权限。 AWS
- 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。
- 亚马逊弹性容器注册表 (Amazon ECR) — 为与您的 AWS 账户关联的亚马逊 ECR 资源提供`Describe`权限。
- 亚马逊弹性容器服务 (亚马逊 ECS) — 为与您的 AWS 账户关联的亚马逊 ECS 资源提供`Describe`权限。
- 亚马逊弹性文件系统 (亚马逊 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。

- 亚马逊 EC2 自动扩展 — 列出与您的 AWS 账户关联的 Amazon EC2 Auto Scaling 资源并提供Describe权限。
- 亚马逊 EC2 系统管理器 (SSM) — 为与您的 AWS 账户关联的 SSM 资源提供Describe权限。
- AWS Fault Injection Service (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 文件服务器的亚马逊 FSx (亚马逊 FSx) — 列出与您的账户关联的亚马逊 FSx 资源并提供Describe权限。 AWS
- 亚马逊 RDS — 列出与您的 AWS 账户关联的 Amazon RDS 资源并提供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。
- 亚马逊简单存储服务 (Amazon S3) — 列出与您的 AWS 账户关联的 Amazon S3 资源并提供Describe权限。

> **Note**
>
> 运行评估时，如果有任何缺失的权限需要从托管策略中更新，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，其中列出了缺少的权限，并将提供一个宽限期来添加相同的权限。如果您没有在指定的宽限期内添加缺失的权限，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 资源并提供Describe权限。
- Directory Service — 列出与您的 AWS 账户关联的 Directory Service 资源并提供Describe权限。
- AWS 弹性灾难恢复 （弹性灾难恢复）-为与您的 AWS 账户关联的弹性灾难恢复资源提供Describe权限。
- AWS Lambda (Lambda) — 列出与您的 AWS 账户关联的 Lambda 资源并提供Describe权限。

- AWS Resource Groups （资源组）-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 （服务目录）-列出与您的 AWS 账户关联的服务目录资源并提供`Describe`权限。
- AWS Step Functions — 列出与您的 AWS 账户关联的 AWS Step Functions 资源并提供`Describe`权限。
- 弹性负载均衡-列出与您的 AWS 账户关联的弹性负载平衡资源并提供`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 政策为用户、用户组和角色添加权限，为您的团队提供在运行评估时访问 AWS 服务所需的权限。

AWS Resilience Hub 更新到 AWS 托管策略

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。要自动收到有关此页面更改的警报，请订阅 “ AWS Resilience Hub 文档历史记录” 页面上的 RSS 提要。

更改	描述	日期
AWSResilienceHubAssessmentExecutionPolicy – 更改	AWS Resilience Hub 更新了授`AWSResilienceHubAssessmentExecutionPolicy` 予`List`和`Get`权限，允许您在运行评估 AWS FIS 时访问实验。	2024 年 12 月 17 日
AWSResilienceHubAssessmentExecutionPolicy – 更改	AWS Resilience Hub 更新了`AWSResilienceHubAssessmentExecutionPolicy` 以授予`Describe`权限，允许您在运行评估时访问亚马逊 ElastiCache (Redis OSS) 无服务器上的资源和配置。	2024 年 9 月 25 日

更改	描述	日期
AWSResilienceHubAssessmentExecutionPolicy – 更改	AWS Resilience Hub 更新了AWSResilienceHubAssessmentExecutionPolicy 以授予Describe权限，允许您在运行评估 AWS Lambda 时访问 Amazon DocumentDB、弹性负载平衡上的资源和配置。	2024 年 8 月 1 日
AWSResilienceHubAssessmentExecutionPolicy – 更改	AWS Resilience Hub 更新了AWSResilienceHubAssessmentExecutionPolicy 以授予Describe权限，允许您在运行评估时读取适用于 Windows 文件服务器的 Amazon FSx 配置。	2024 年 3 月 26 日
AWSResilienceHubAssessmentExecutionPolicy – 更改	AWS Resilience Hub 更新了AWSResilienceHubAssessmentExecutionPolicy 以授予Describe权限，允许您在运行评估时读取 AWS Step Functions 配置。	2023 年 10 月 30 日
AWSResilienceHubAssessmentExecutionPolicy – 更改	AWS Resilience Hub 更新AWSResilienceHubAssessmentExecutionPolicy 为授予Describe权限，允许您在运行评估时访问 Amazon RDS 上的资源。	2023 年 10 月 5 日
AWSResilienceHubAssessmentExecutionPolicy—全新	此 AWS Resilience Hub 政策提供对其他 AWS 服务进行评估的访问权限。	2023 年 6 月 26 日

更改	描述	日期
AWS Resilience Hub 已开始跟踪更改	AWS Resilience Hub 开始跟踪其 AWS 托管策略的更改。	2023 年 6 月 15 日

AWS Resilience Hub 角色和 IAM 权限参考

您可以使用AWSResilienceHubAsssessmentExecutionPolicy AWS 托管策略和以下特定角色策略之一向需要 AWS Resilience Hub 使用的角色授予 IAM 权限。有关 AWS 托管策略的更多信息，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

以下人员建议的角色政策： AWS Resilience Hub

- 基础设施应用程序管理员角色的 IAM 权限
- 业务连续性经理角色的 IAM 权限
- 应用程序所有者角色的 IAM 权限
- 授予只读访问权限的 IAM 权限

基础设施应用程序管理员角色的 IAM 权限

以下策略授予了基础架构应用程序管理员角色所需的必要权限。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "InfrastructureApplicationManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
```

```
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource"
      ],
      "Resource": "*"
    }
  ]
}
```

业务连续性经理角色的 IAM 权限

以下策略授予业务连续性经理角色所需的必要权限。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "BusinessContinuityManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
```

```
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

应用程序所有者角色的 IAM 权限

以下政策授予应用程序所有者角色所需的必要权限。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ApplicationOwner",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:BatchUpdateRecommendationStatus",
        "resiliencehub:CreateApp",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteApp",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:ImportResourcesToDraftAppVersion",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
```

```
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateApp",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

授予只读访问权限的 IAM 权限

以下策略授予只读访问权限所需的必要权限。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources"
      ],
      "Resource": "*"
    }
  ]
}
```

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 () 或托管密钥 (SSE-S3) 加密的 Terraform 状态文件。 AWS Key Management Service SSE-KMS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，则您将无法使用导入它们。 AWS Resilience Hub

将 Terraform 状态文件导入到 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。
- 身份策略-为此应用程序定义的调用者角色的关联身份策略，或主 AWS 账户 AWS Resilience Hub 上的 AWS 当前 IAM 角色。有关更多信息，请参阅以下示例。

  JSON

```
{
  "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。
- 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。

> **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>"
}
```

正在启用 AWS Resilience Hub 访问您的亚马逊 Elastic Kubernetes 服务集群

AWS Resilience Hub 通过分析您的亚马逊 EKS 集群的基础设施，评估亚马逊弹性 Kubernetes 服务（亚马逊 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 (K8s) 工作负载，这些工作负载是作为亚马逊 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。

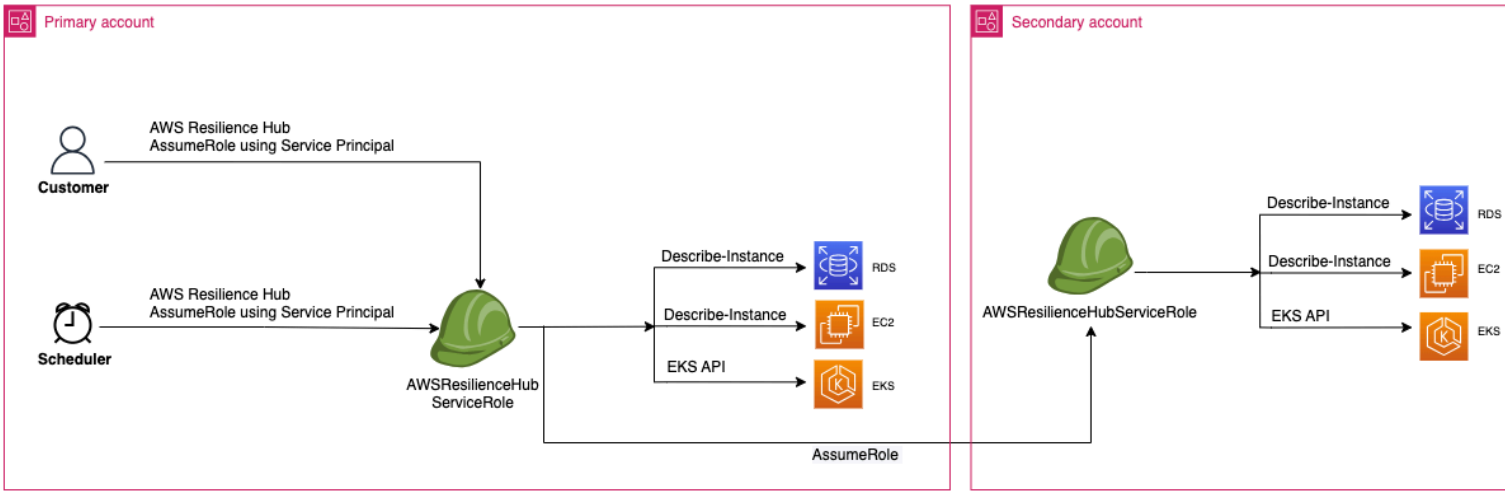
> **Note**
>
> - 有关所有`aws-auth ConfigMap`设置的更多信息，请参阅上的完整配置格式 GitHub。
> - 有关不同 IAM 实体的更多信息，请参阅 IAM 用户指南中的身份（用户、组和角色）。
> - 有关基于 Kubernetes 角色访问控制（RBAC）配置的更多信息，请参阅使用 RBAC 授权。

AWS Resilience Hub 使用账户中的 IAM 角色查询亚马逊 EKS 集群内的资源。 AWS Resilience Hub 要访问您的亚马逊 EKS 集群中的资源， AWS Resilience Hub 必须将使用的 IAM 角色映射到 Kubernetes 群组，该群组对亚马逊 EKS 集群内的资源具有足够的只读权限。

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：

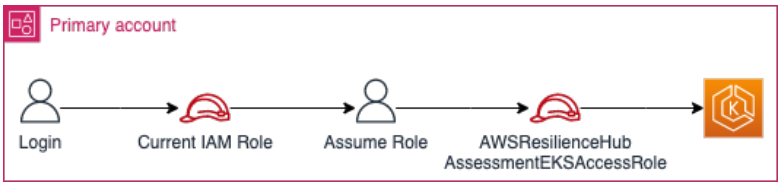
- 如果您的应用程序配置为使用基于角色的访问权限来访问资源，则在评测期间，将使用在创建应用程序时传递到 AWS Resilience Hub 的调用者角色或辅助账户角色访问您的 Amazon EKS 集群。

  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。

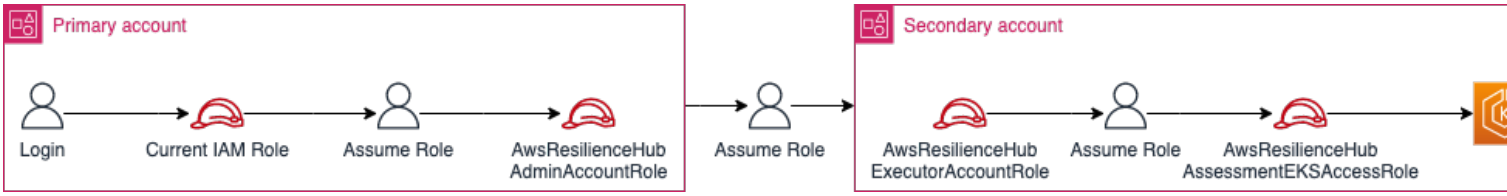


- 如果您的应用程序配置为使用当前 IAM 用户访问资源，则必须在与 Amazon EKS 集群相同的账户中创建一个名为 `AwsResilienceHubAssessmentEKSAccessRole` 的新的 IAM 角色。然后，此 IAM 角色将用于访问您的 Amazon EKS 集群。

  以下概念图显示了将应用程序配置为使用当前 IAM 用户权限时，如何 AWS Resilience Hub 访问在您的主账户中部署的 Amazon EKS 集群。



  以下概念图显示了将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 AWS Resilience Hub 访问您的 Amazon EKS 集群中的资源

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

向授予所需的权限 AWS Resilience Hub 用于发现和评估 Amazon EKS 集群中的资源

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 “操作方法 AWS 弹性中心可与 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。此角色应在与您的亚马逊 EKS 集群相同的账户中创建，并将映射到一个 Kubernetes 群组，该群组包含评估您的亚马逊 EKS 集群所需的权限。 AWS Resilience Hub

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的 API AWS Resilience Hub。

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

如果您的 Amazon EKS 集群处于跨账户（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，必须配置多账户访问权限。有关更多信息，请参阅

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作 AWS Resilience Hub 为 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，必须创建以下和。`ClusterRole` `ClusterRoleBinding`

- `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — 定义评估您的亚马逊 EKS 集群所需的权限。 AWS Resilience Hub
- `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
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
```

```
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. 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 集群内特定命名空间中的资源并评估其弹性，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— 指定评估您的 Amazon EKS 集群内集群范围内的资源所需的权限，这些资源与特定命名空间无关。 AWS Resilience Hub 需要访问您的 Amazon EKS 集群上的集群范围资源（例如节点）的权限，以评估应用程序的弹性。

  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
      - nodepools
    verbs:
      - get
```

```
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
      - ec2nodeclasses
    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中的资源。

> **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）。
> 这样，您将授予 AWS Resilience Hub 在评估您的 Amazon EKS 集群时评估kube-system命名空间内资源所需的权限。

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 AWS Resilience Hub 访问集群范围资源所需的权限。

  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，则该角色应是创建应用程序 AWS Resilience Hub 时传递给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应该是亚马逊 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
```

正在启用 AWS Resilience Hub 发布到您的亚马逊简单通知服务主题

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) 主题发布有关应用程序的通知。要向 Amazon SNS 主题推送通知，请确保您具备以下条件：

- 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。

要启用 AWS Resilience Hub 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：

> **Note**
>
> 当您使用 AWS Resilience Hub 将消息从选择加入区域发布到位于默认启用的区域中的主题时，必须修改为 Amazon SNS 主题创建的资源政策。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，必须包括以下 AWS Key Management Service 访问策略权限。

限制权限以包含或排除 AWS Resilience Hub 建议

AWS Resilience Hub 允许您限制权限以包含或排除每个应用程序的推荐。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）用于在当前账户中调用 API AWS Resilience Hub。

中的基础设施安全 AWS Resilience Hub

作为一项托管服务 AWS Resilience Hub ，受《亚马逊网络服务：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。我们建议使用 TLS 1.3 或更高版本。客户还必须支持具有完全向前保密 (PFS) 的密码套件，例如短暂的 (DHE) 或椭圆曲线短暂的 Diffie-Hellman (ECDHE)。 Diffie-Hellman 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 主体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。

弹性检查 AWS 务

本章详细介绍了对支持的 AWS 服务执行的各种弹性检查，以确保应用程序的弹性状态不受影响。AWS Resilience Hub 这些检查根据每个应用程序组件的弹性策略中定义的值来估算恢复时间目标 (RTO) 和恢复点目标 (RPOAppComponent) ()。评估涵盖不同类型的中断，即应用程序、基础设施故障、AZ 中断和区域故障。但是，要运行这些检查，您必须向提供相关的 IAM 权限， AWS Resilience Hub 以允许其访问您的资源。要详细了解本章中 AWS Resilience Hub 允许访问您的资源和执行弹性检查所需的 IAM 权限，请参阅AWS 的托管策略 AWS Resilience Hub。

AWS 服务

- Amazon Elastic File System
- 亚马逊关系数据库服务和亚马逊 Aurora
- Amazon Simple Storage Service
- Amazon DynamoDB
- Amazon Elastic Compute Cloud
- Amazon EBS
- AWS Lambda
- Amazon Elastic Kubernetes Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Elastic Container Service
- Elastic Load Balancing

- Amazon API Gateway
- Amazon DocumentDB
- NAT 网关
- Amazon Route 53
- Amazon 应用程序恢复控制器（ARC）
- 适用于 Windows File Server 的 Amazon FSx
- AWS Step Functions
- 亚马逊 ElastiCache （Redis OSS）

Amazon Elastic File System

本节列出了所有特定于亚马逊弹性文件系统的弹性检查和建议。有关亚马逊弹性文件系统的更多信息，请参阅亚马逊弹性文件系统文档。

文件系统类型

AWS Resilience Hub 检查文件系统类型：区域或单区域。在基础设施或可用区发生中断时，文件系统类型会影响其弹性。有关文件系统类型的更多信息，请参阅 Amazon EFS 文件系统的可用性和耐久性。

文件系统备份

AWS Resilience Hub 检查是否为已部署的文件系统定义了 AWS Backup 计划。此外，它还会验证`Cross-Region`备份选项是否已启用，确保在政策要求时覆盖 Region-level 中断。

数据复制

AWS Resilience Hub 检查是否为已部署的文件系统定义了区域内或跨区域 Amazon EFS 数据复制。Amazon EFS 数据复制有助于提高应用程序、基础设施、可用区和区域级别的预计 RTO 和预计 RPO。此外， AWS Resilience Hub 检查它是否与区域内文件相结合 AWS Backup ，以在应用程序中断时实现文件系统灵活性。

亚马逊关系数据库服务和亚马逊 Aurora

本部分列出了针对亚马逊关系数据库服务和亚马逊 Aurora 的所有弹性检查和建议。有关亚马逊关系数据库服务和亚马逊 Aurora 的更多信息，请参阅亚马逊关系数据库服务文档。

Single-AZ 部署

AWS Resilience Hub 检查数据库是否作为单个实例部署，如果确定，则表明它不支持辅助实例和只读副本。

Multi-AZ 部署

AWS Resilience Hub 检查数据库是使用辅助实例还是只读副本进行部署。如果使用只读副本部署数据库，则 AWS Resilience Hub 验证其是否部署在不同的可用区，以允许在可用区中断时进行故障转移。

备份

AWS Resilience Hub 检查已部署的数据库实例上是否应用了以下备份功能。

- AWS Backup 使用自动备份选项进行规划
- AWS Backup 如果您的政策要求，请使用跨区域备份副本进行规划
- 第三方备份系统的手动快照

Cross-Region 故障转移

AWS Resilience Hub 检查灵活性策略中定义的 RTO 和 RPO 目标，以从区域中断中恢复过来。此外，AWS Resilience Hub 可以确定以下跨区域架构以应对区域中断：

- 带有跨区域快照副本的区域内备份
- 另一个区域的只读副本
- 一个 Amazon Aurora 全球数据库，其辅助集群位于另一个区域
- Amazon Aurora 全球数据库，在另一个区域具有无头辅助集群

更快的区域内故障转移

AWS Resilience Hub 检查基础设施或可用区中断期间弹性策略中定义的 RTO 和 RPO 目标。此外，AWS Resilience Hub 可以确定以下区域内架构以应对应用程序、基础设施和可用区中断：

- 备 In-Region 份
- 不同可用区中的只读副本
- 在另一个 AZ 中有只读副本的 Aurora 集群
- 亚马逊关系数据库服务 (Amazon RDS) 的 Multi-AZ 实例

- 亚马逊 RDS Multi-AZ 集群
- 一个 Amazon RDS 实例，其只读副本位于另一个可用区

Amazon Simple Storage Service

本节列出了针对亚马逊简单存储服务 (Amazon S3) 的所有弹性检查和建议。有关 Amazon S3 的更多信息，请参阅 Amazon S3 文档。

版本控制

AWS Resilience Hub 验证 Amazon S3 存储桶是否配置了启用版本控制。

定时备份

AWS Resilience Hub 检查是否为已部署的亚马逊简单存储服务 (Amazon S3) 存储桶定义了 AWS Backup 计划。此外，如果您的政策要求提供中 Region-level 断保障，它还会检查是否启用了跨区域备份选项。

Point-in-time 恢复

AWS Resilience Hub 检查您的弹性策略的 RPO 目标是否需要时间点恢复 (PITR)。但是，PITR 不支持跨区域备份。因此，您可以使用启用跨区域备份选项的现有 AWS Backup 计划计划，或者创建一个新的计划。

数据复制

AWS Resilience Hub 检查是否为已部署的 Amazon S3 存储桶定义了同区域复制 (SRR) 和跨区域复制 (CRR)。Amazon S3 数据复制改善了应用程序、基础设施、可用区和区域级别的预计工作负载 RTO 和预计工作负载 RPO。此外，它还可以防止对象被物理删除，因为删除对象版本不会复制到目标 Amazon S3 存储桶。此外，根据您的弹性策略中定义的 RTO 目标， AWS Resilience Hub 检查是否应启用 Amazon S3 复制时间控制 (S3 RTC)。此计费功能可在 15 分钟内复制 99.99% 的源存储桶对象。

- AWS Backup 使用自动备份选项进行规划
- AWS Backup 如果您的政策要求，请使用跨区域备份副本进行规划
- 第三方备份系统的手动快照

Amazon DynamoDB

本部分列出了所有特定于 Amazon DynamoDB 的弹性检查和建议。有关亚马逊 DynamoDB 的更多信息，请参阅亚马逊 DynamoDB 文档。

定时备份

AWS Resilience Hub 检查是否已经为部署的表定义了备份。此外，如果需要中 Region-level 断保障，它还会检查是否应为您的策略配置跨区域备份。

Point-in-time 恢复

AWS Resilience Hub 根据您的弹性策略的 RPO 目标，检查是否需要时间点恢复 (PITR)。但是，PITR 不支持跨区域备份。因此，您可以使用启用跨区域备份选项的现有 AWS Backup 计划计划，或者创建一个新的计划。

全局表

AWS Resilience Hub 检查已部署的 Amazon DynamoDB 表是否被定义为一个在其他区域具有一个或多个副本的全局表。设置 Global Table 可以改善区域级别的估计工作负载 RTO 和估计的工作负载 RPO，还提供了在主动-主动或主动-被动多区域模式下工作的能力。 AWS Backup 或者可以在其中一个地区使用亚马逊 DynamoDB PITR 来处理应用程序中断。

Amazon Elastic Compute Cloud

本部分列出了针对亚马逊弹性计算云的所有弹性检查和建议。有关亚马逊弹性计算云的更多信息，请参阅亚马逊弹性计算云文档。

有状态实例

AWS Resilience Hub 如果满足以下条件之一，则将 Amazon EC2 实例标识为有状态实例：

- 如果将至少一个连接到该实例的亚马逊弹性区块存储（亚马逊 EBS）卷的`DeleteOnTermination`属性设置为 false。
- 如果亚马逊数据生命周期管理器或 AWS Backup 计划已连接到亚马逊 EC2 实例或至少一个 Amazon EBS 卷。
- AWS 弹性灾难恢复 它用于复制您的 Amazon EC2 实例存储卷。

> **Note**
>
> 如果亚马逊 EC2 实例不符合上述任何标准，则将其 AWS Resilience Hub 视为无状态的 Amazon EC2 实例。

自动扩缩组

AWS Resilience Hub 检查一组无状态的亚马逊 EC2 实例。如果被发现，建议使用带配置的 Auto Scaling 组 (ASG) 进行 Multi-AZ编排。如果确定了现有 ASG，ARH 将验证其配置是否跨多个可用区。如果也仅使用竞价型亚马逊 EC2 实例定义 ASG，则建议使用按需亚马逊 EC2 实例来增强其容量，以提高竞价亚马逊 EC2 实例不可用时的弹性。

亚马逊 EC2 舰队

AWS Resilience Hub 识别亚马逊 EC2 队列并验证它是否被定义为 Multi-AZ部署，以及它是否仅使用亚马逊 EC2 竞价实例。将 Amazon EC2 队列定义为 Multi-AZ 部署将提高其在可用区中断时的灵活性。在竞价型实例不可用时，使用按需实例增强 Amazon EC2 队列将提高其灵活性。

Amazon EBS

本节列出了所有特定于 Amazon EBS 的弹性检查和建议。有关亚马逊 EBS 的更多信息，请参阅亚马逊 EBS 文档。

定时备份

AWS Resilience Hub 检查是否为您的亚马逊 EBS 卷定义了以下一项或两项。

- 连接到您的亚马逊 EC2 实例的特定亚马逊 EBS 卷的备份规则。
- 为您的亚马逊 EC2 实例创建 Amazon EBS-backed AMI 的备份规则。
- 第三方备份系统的手动快照。

此外，如果您的政策要求为 Region-level 中断提供保障，请 AWS Resilience Hub 检查您的备份规则是否启用了跨区域备份选项。

数据备份和复制

AWS Resilience Hub 确定如果满足以下条件之一，则 Amazon EBS 卷被视为有状态卷：

- 如果将此亚马逊 EBS 卷的`DeleteOnTermination`属性设置为 false。

- 如果亚马逊数据生命周期管理器或 AWS Backup 计划与此 Amazon EBS 卷或其连接的 Amazon EC2 实例相关联。
- AWS 弹性灾难恢复 它用于复制您的 Amazon EC2 实例存储卷。

AWS Lambda

本节列出了所有针对的弹性检查和建议 AWS Lambda。有关的更多信息 AWS Lambda，请参阅AWS Lambda 文档。

客户亚马逊 VPC 访问权限

AWS Resilience Hub 标识连接到 VPC 的 AWS Lambda 函数。连接 AWS Lambda 到 Amazon VPC 不同可用区中的子网可在可用区中断时保持功能灵活性。

Dead-letter 队列

AWS Resilience Hub 检查 AWS Lambda 函数是否附有用于存储失败请求的死信队列 (DLQ)。将 DLQ 附加到 AWS Lambda 函数可以防止请求的数据丢失，并在以后重试处理失败的请求。

Amazon Elastic Kubernetes Service

本节列出了所有特定于亚马逊弹性Kubernetes服务（亚马逊 EKS）的弹性检查和建议。有关亚马逊 EKS 的更多信息，请参阅亚马逊 EKS 文档。

Multi-AZ 部署

AWS Resilience Hub 识别 pod 部署是否在多个可用区的多个工作节点上运行。如果您的弹性政策要求在发生区域中断时提供保障，则需要在另一个地区额外增加一个 Amazon EKS 集群。这个额外的 Amazon EKS 集群还经过验证，适用于分布在多个可用区的多个工作节点之间的 pod 部署。

部署 vs. ReplicaSet

AWS Resilience Hub 检查你是否使用 ReplicaSets 或 pod 对象而不是部署。使用部署替换 ReplicaSets 或 pod 对象可简化对新版本软件的 pod 更新，并包含其他有用的功能。

部署维护

AWS Resilience Hub 检查是否使用以下最佳实践进行部署：

- 使用 Pod 中断预算 (PDB) — 使用 PDB 可以设置工作负载中可在任何给定时间中断的 Pod 数量的限制，从而提高可用性。

- 用 Amazon EKS 托管节点组替换自我管理的节点组 — 这种替代方案简化了维护期间的工作节点映像更新。
- 支持每次部署的动态 CPU 和内存请求 — 这些请求有助于 Kubernetes 选择适合容器需求的节点。
- 为所有容器配置存活和就绪探测器 — 配置存活探针有助于通过重启非功能的 pod 来提高弹性。配置就绪探测器可以将流量从繁忙的 pod 中转移出去，从而提高可用性。
- 配置 Karpenter、集群自动扩缩器或 AWS Fargate — 这些配置允许 Amazon EKS 集群的基础设施增长并满足工作负载需求。
- 配置水平 Pod 自动扩缩器 — 此配置可帮助 Amazon EKS 集群自动扩展工作负载以满足请求处理需求。

Amazon Simple Notification Service

本节列出了所有特定于亚马逊简单通知服务 (Amazon SNS) 的弹性检查和建议。有关亚马逊 SNS 的更多信息，请参阅亚马逊 SNS 文档。

话题订阅

AWS Resilience Hub 检查 Amazon SNS 主题是否有至少 1 个订阅，以确保传入的消息不会丢失。

Amazon Simple Queue Service

本节列出了所有特定于亚马逊简单队列服务 (Amazon SQS) 的弹性检查和建议。有关亚马逊 SQS 的更多信息，请参阅亚马逊 SQS 文档。

Dead-letter 队列

AWS Resilience Hub 检查 Amazon SQS 队列是否有与之关联的 DLQ 来处理无法成功传送给订阅者的消息。

Amazon Elastic Container Service

本节列出了针对亚马逊弹性容器服务 (Amazon ECS) 的所有弹性检查和建议。有关亚马逊 ECS 的更多信息，请参阅亚马逊 ECS 文档。

Multi-AZ 部署

AWS Resilience Hub 根据亚马逊 EC2 或 AWS Fargate 启动类型检查亚马逊 ECS 任务或服务是否在多个可用区中运行。如果您的保单需要为区域中断提供保障，则需要在另一个地区额外部署一个 Amazon ECS 集群。另外的集群还经过验证，可以在多个可用区中执行任务或服务。

Elastic Load Balancing

本节列出了所有特定于弹性负载平衡的弹性检查和建议。有关弹性负载平衡的更多信息，请参阅弹性负载平衡文档。

Multi-AZ 部署

AWS Resilience Hub 检查弹性负载平衡是否在多个可用区中运行。

如果您的政策需要为区域中断提供保障，则需要在其他地区进行额外的弹性负载均衡。位于不同区域的额外弹性负载均衡还经过验证，可在多个可用区中部署。

Amazon API Gateway

本节列出了所有特定于亚马逊 API Gateway 的弹性检查和建议。有关亚马逊 API 网关的更多信息，请参阅亚马逊 API 网关文档。

Cross-Region 部署

如果您的政策需要考虑区域干扰， AWS Resilience Hub 将检查是否在其他地区额外部署了 Amazon API Gateway API 资源。

私有 API Multi-AZ 部署

AWS Resilience Hub 检查您的 API 在亚马逊 API 网关中是否被定义为私有 API。私有 API 应通过部署到多个可用区的亚马逊 VPC 接口终端节点接收流量。

Amazon DocumentDB

本部分列出了所有特定于 Amazon DocumentDB 的检查和建议。有关 Amazon DocumentDB 的更多信息，请参阅亚马逊 DocumentDB 文档。

Multi-AZ 部署

AWS Resilience Hub 检查 Amazon DocumentDB 集群是否部署在多个可用区中。如果您的政策要求为区域中断提供保障，则需要在其他地区增加一个 Amazon DocumentDB 二级集群。位于不同区域的额外Amazon DocumentDB集群也经过验证，可在多个可用区中执行。

弹性集群和 Multi-AZ 部署

AWS Resilience Hub 检查 Amazon DocumentDB 弹性集群分片是否使用部署在不同可用区的只读副本。

弹性集群和手动快照

AWS Resilience Hub 检查是否定期为 Amazon DocumentDB 弹性集群创建手动快照。手动快照可延长保存时间，并可灵活设置快照频率以满足您的业务需求。

NAT 网关

本节列出了所有特定于 NAT 网关的检查和建议。有关 NAT 网关的更多信息，请参阅 NAT 网关。

Multi-AZ 部署

AWS Resilience Hub 检查 NAT 网关是否部署在多个可用区中。如果您的政策要求承保区域中断，则需要在其他地区额外部署 NAT 网关。位于不同区域的额外 NAT 网关还经过验证，可在多个可用区中部署。

Amazon Route 53

本部分列出了针对亚马逊 Route 53 的所有检查和建议。有关亚马逊 Route 53 的更多信息，请参阅亚马逊 Route 53 文档。

Multi-AZ 部署

AWS Resilience Hub 检查 Amazon Route 53 托管区域记录是否定义为在同一区域中有多个目标，以及这些目标是否部署在多个可用区中。如果您的政策要求为区域中断提供保障，请 AWS Resilience Hub 检查 Amazon Route 53 托管区域记录是否在多个区域中定义，每个区域有多个目标，以及这些目标是否部署在多个可用区中。

Amazon 应用程序恢复控制器（ARC）

本节列出了针对亚马逊应用程序恢复控制器 (ARC) (ARC) 的所有检查和建议。有关 ARC 的更多信息，请参阅 ARC 文档。

Multi-AZ 部署

AWS Resilience Hub 检查是否在多个区域部署了类似资源，并建议将 ARC 准备情况检查定义为最佳实践，以提高区域中断时的可用性和就绪程度。您将收到通知，您将产生额外的每小时费用。

适用于 Windows File Server 的 Amazon FSx

本部分列出了针对适用于 Windows 文件服务器的 Amazon FSx 的所有检查和建议。有关适用于 Windows 文件服务器的亚马逊 FSx 的更多信息，请参阅适用于 Windows 的亚马逊 FSx 文件服务器文档。

文件系统类型

AWS Resilience Hub 检查文件系统类型：`Regional`或`One Zone`。在基础设施或可用区发生中断时，文件系统类型会影响其弹性。有关文件系统类型的更多信息，请参阅 Amazon EFS 。

文件系统备份

AWS Resilience Hub 检查是否 AWS Backup 为已部署的文件系统定义了。此外，如果您的保单要求承保 Region-level中断，它还会检查该`cross-Region backup`选项是否已启用。

数据复制

AWS Resilience Hub 检查是否为已部署的文件系统定义了区域内或跨区域定时 AWS DataSync 数据复制任务。

AWS DataSync 定期数据复制任务可以改善基础架构、AZ 和区域级别的预估工作负载 RTO 和预计工作负载 RPO。此外，它可以与区域内结合使用 AWS Backup ，以便在应用程序中断时恢复。

AWS Step Functions

本节列出了所有特定于的检查和建议 AWS Step Functions。有关的更多信息 AWS Step Functions，请参阅AWS Step Functions 文档。

版本控制和别名

AWS Resilience Hub 检查 AWS Step Functions 工作流程是否使用版本控制和别名来缩短重新部署时间。

Cross-Region 部署

AWS Resilience Hub 检查相同 AWS Step Functions 工作流程类型的工作流是否部署在不同的区域，以便在区域中断时恢复。

亚马逊 ElastiCache （Redis OSS）

本部分列出了针对亚马逊 ElastiCache (Redis OSS) 的所有检查和建议。

有关亚马逊 ElastiCache （Redis OSS）的更多信息，请参阅亚马逊 ElastiCache 文档。

Single-AZ 部署

AWS Resilience Hub 检查亚马逊 ElastiCache （Redis OSS）集群是作为单个节点部署还是将其所有节点部署在单个可用区中。

Single-AZ 部署

AWS Resilience Hub 验证 Amazon ElastiCache (Redis OSS) 集群是否作为复制组（适用于已启用集群模式和禁用集群模式的集群）跨多个可用区部署，以允许在可用区中断时进行故障转移。

Cross-Region 故障转移

AWS Resilience Hub 检查弹性策略中定义的 RTO 和 RPO 目标，以从区域中断中恢复过来。此外，AWS Resilience Hub 可以识别部署在多个区域的亚马逊 ElastiCache （Redis OSS）全球数据存储集群。

备份

AWS Resilience Hub 检查已部署的 Amazon ElastiCache (Redis OSS) 或自行设计的集群上是否应用了以下备份功能：

- 自动备份
- 手动备份第三方备份系统

AWS Resilience Hub 如果您不使用备份，则不建议将备份作为恢复方法。但是，如果数据不一致，您可以重置缓存层，并从主存储器重新创建数据。

更快的区域内故障转移

AWS Resilience Hub 检查基础设施或可用区中断期间弹性策略中定义的 RTO 和 RPO 目标。此外，AWS Resilience Hub 可以识别以下区域内架构，以从基础设施和可用区中断中恢复过来：

- 禁用集群模式的不同可用区域中的辅助备用节点实例 ElastiCache （Amazon (Redis OSS) 集群。
- 对于启用集群模式的 Amazon ElastiCache (Redis OSS) 集群，每个分片位于不同的可用区中的辅助备用节点实例。

使用其他服务

本节介绍与交互的 AWS 服务 AWS Resilience Hub。

主题

- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- AWS Trusted Advisor

AWS CloudFormation

AWS Resilience Hub 与一项服务集成 AWS CloudFormation，该服务可帮助您对 AWS 资源进行建模和设置，从而减少创建和管理资源和基础架构所花费的时间。您可以创建一个描述所需的所有 AWS 资源（例如 AWS::ResilienceHub:::ResiliencyPolicy 和 AWS::ResilienceHub:::App）的模板，然后为您 CloudFormation 预置和配置这些资源。

使用时 CloudFormation，您可以重复使用模板来一致且重复地设置 AWS Resilience Hub 资源。一次描述您的资源，然后在多个 AWS 账户和区域中重复配置相同的资源。

AWS Resilience Hub 和 CloudFormation 模板

要为和相关服务配置 AWS Resilience Hub 和配置资源，必须了解CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述了您要在 CloudFormation 堆栈中配置的资源。如果你不熟悉 JSON 或 YAML，可以使用 D CloudFormation esigner 来帮助你开始使用 CloudFormation 模板。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的什么是 CloudFormation Designer？。

AWS Resilience Hub 支持创建 AWS::ResilienceHub:::ResiliencyPolicy 和输 AWS::ResilienceHub:::App入 CloudFormation。有关更多信息，包括和的 JSON 和 YAML 模板示例 AWS::ResilienceHub:::App，请参阅AWS CloudFormation 用户指南中的AWS Resilience Hub 资源类型参考。 AWS::ResilienceHub:::ResiliencyPolicy

您可以使用 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。

了解更多关于 CloudFormation

有关的更多信息 CloudFormation，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- CloudFormation API 引用
- 《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 AWS Resilience Hub 对 API 操作的代码调用。如果您创建跟踪，则可以启用向 Amazon S3 存储桶持续交付事件，包括的事件 AWS Resilience Hub。 CloudTrail 如果您未配置跟踪，仍可以在 CloudTrail 控制台的事件历史记录中查看最新事件。使用收集的信息 CloudTrail，您可以确定向谁发出了请求 AWS Resilience Hub、发出请求的 IP 地址、谁提出了请求、何时提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 配合使用，通过提供大量可用作这些标准操作基础的 SSM 文档，自动执行标准操作步骤。

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 CloudFormation 模板，每个文档都有一个角色，具有特定文档所需的权限。使用 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，以便系统管理器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 管理标准操作程序。

AWS Trusted Advisor

AWS Trusted Advisor 是 AWS 最佳实践建议的集中存放处，可帮助您识别、优先考虑和优化部署 AWS。 AWS Trusted Advisor 检查您的 AWS 环境，然后通过检查提出建议，以节省资金、提高系统可用性和性能或帮助弥合安全漏洞。这些支票根据其目的分为多个类别。有关不同签入类别的更多信息 AWS Trusted Advisor，请参阅AWS 支持用户指南。

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，提供多个高级灵活性建议。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。当出现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 故障和政策违规时，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，这些建议将增加降低这些风险的机会，该部分需要在中 AWS Resilience Hub介绍。要详细了解中每个应用程序的推荐 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以下检查 AWS Resilience Hub：

- AWS Resilience Hub 应用程序弹性分数 — 检查应用程序的最新评估中的弹性分数， AWS Resilience Hub 并在其弹性分数低于特定值时提醒您。

  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 到 69 之间。
  - 红色 -表示您的应用程序的弹性分数低于 40。

  建议采取的行动

  为了改善应用程序的弹性状况并尽可能获得最佳的弹性分数，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 including/excluding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 “在中进行弹性评估 AWS Resilience Hub”
  - 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 -检查应用程序是否满足您为 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 目标时提醒您。

  警报标准

  - 绿色 — 表示应用程序有策略，预计工作负载 RTO 和预计工作负载 RPO 达到 RTO 和 RPO 目标。
  - 黄色 -表示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，预计工作负载 RTO 和预计工作负载 RPO 未达到 RTO 和 RPO 目标。

  建议采取的行动

为确保应用程序的预估工作负载 RTO 和预计的工作负载 RPO 仍符合定义的 RTO 和 RPO 目标，请使用应用程序资源的最新更新版本定期进行评估。此外，如果您想确保不违反应用程序的弹性政策，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 每日代表您进行评估、运行评估、审查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 要启用每天代表您进行评估，请完成编辑申请程序的偏差通知设置中的步骤，选中 “自动每日评估” 复选框。 ）
- the section called “在中进行弹性评估 AWS Resilience Hub”
- 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 — 检查自上次对中的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过评估。

  建议采取的行动

  定期进行评估，以管理和改善应用程序的弹性状况 AWS。如果您 AWS Resilience Hub 想代表自己每天评估您的应用程序，则可以通过在 AWS Resilience Hub 偏移通知中选中 “每天自动评估此应用程序” 复选框来启用该功能。要选中 “每天自动评估此应用程序” 复选框，请在中填写 “编辑申请程序的偏差通知” ???。

  > **Note**
  >
  > 该检查仅确定至少经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 AppComponent 无法恢复，则可能会遇到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。

  建议采取的行动

  为确保您的 AppComponent 可恢复，请审查并实施弹性建议，然后进行新的评估。有关审查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 支持 用户指南。

的文档历史记录 AWS Resilience Hub 用户指南

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 12 月 17 日

变更	说明	日期
添加了 EventBridge 通知事件	下一代 Resilience Hub 现在向亚马逊发送事件，以 EventBridge 进行评估生命周期、故障模式寻找解决方案和新的依赖关系发现。您可以创建 EventBridge 规则来自动响应这些事件。有关更多信息，请参阅EventBridge 通知。	2026 年 7 月 9 日
记录在案的依赖关系发现状态字段	添加了`DependencyDiscoveryConfig` 响应结构中`eligibleResourceCount` 和`message`字段的文档。这些字段允许您通过`GetService` 和`ListServices` API 操作监控依赖项发现的状态。	2026 年 6 月 30 日
增加了弹性测试 IAM 权限	为 AWS Fault Injection Service 假定运行弹性测试的 IAM 执行角色添加了信任和权限策略，包括单账户和多账户测试。	2026 年 6 月 15 日
增加了弹性测试	添加了弹性测试文档，允许您使用基于 AWS Fault Injection	2026 年 6 月 4 日

	Service的预配置测试来验证服务恢复。	
新一代 Resilience Hub 用户指南的首次发布	新一代 Resilence Hub 用户指南的初始版本。	2026 年 5 月 19 日
AWS Resilience Hub 集成了已经实施的亚马逊 CloudWatch 警报	AWS Resilience Hub 现在可以自动检测已配置的 Amazon CloudWatch 警报并将其集成到其弹性评估中，从而更全面地了解您的应用程序的弹性状况。这项新功能将 AWS Resilience Hub 建议与您当前的监控设置相结合，以简化警报管理并提高评估准确性。 有关更多信息，请参阅 管理警报。	2024 年 12 月 17 日

AWS Resilience Hub 支持通过量身定制的 AWS Fault Injection Service 实验提供简化的弹性测试的额外功能	AWS Resilience Hub 现在支持增强与 AWS Fault Injection Service (AWS FIS) 的集成，使用基于特定应用程序环境的 AWS FIS 操作和场景提供量身定制的建议，以改善弹性状况。运行推荐的实验或您自己的测试将提高您的弹性分数，从而使您能够跟踪一段时间内的变化。 有关更多信息，请参阅以下主题： • AWSResilienceHubAssessmentExecutionPolicy • 管理 AWS Fault Injection Service 实验 • AWS Resilience Hub — 弹性测试	2024 年 12 月 17 日
AWS Resilience Hub 引入摘要视图	AWS Resilience Hub新的摘要视图通过清晰的图表和图表提供了应用程序弹性的高级可视化表示，使您可以直观地了解应用程序组合的状态，并有效地管理和提高应用程序承受中断和恢复的能力。除了新的摘要视图外，您还可以导出支持摘要视图的数据，以创建用于利益相关者沟通的自定义报告。 有关更多信息，请参阅 the section called “AWS Resilience Hub 摘要”。	2024 年 11 月 21 日

AWS Resilience Hub 在 MyApplications 仪表板中引入了弹性控件	MyApplications 仪表板中的新弹性控件可简化对应用程序弹性状况的评估和监控。它使您能够快速评估在 myApplications 中定义的应用程序的弹性，而不必在中手动复制它们。 AWS Resilience Hub 有关更多信息，请参阅以下主题： • the section called “AWS Resilience Hub 和 “我的应用程序”” • the section called “通过弹性小工具管理弹性评估”	2024 年 10 月 22 日

AWS Resilience Hub 扩展对亚马逊 ElastiCache (Redis OSS) 无服务器的支持	AWS Resilience Hub 现在评估使用亚马逊 ElastiCache（Redis OSS）的应用程序，包括亚马逊 ElastiCache（Redis OSS）无服务器和全球数据存储，并提供增强弹性建议。其中包括区域和多区域设置指南，以及 Multi-AZ 部署、资源分组和备份策略。此外，为了更好地控制应用程序的弹性状态， AWS Resilience Hub 提供了专为亚马逊 ElastiCache (Redis OSS) 量身定制的亚马逊 CloudWatch 警报。 有关更多信息，请参阅以下主题： • the section called “管理应用程序组件” • the section called “支持的 AWS Resilience Hub 资源” • the section called “AWSResilienceHubAsssessmentExecutionPolicy”	2024 年 9 月 25 日

AWS Resilience Hub 介绍分组建议	AWS Resilience Hub 引入了新的智能分组选项，可在载入应用程序时将资源分组到应用程序组件 (AppComponents) 中。当您在上进行弹性评估时 AWS Resilience Hub，将资源准确分组为相应的资源非常重要，这样 AppComponents 才能获得经过优化和可操作的建议。此选项非常适合复杂或跨区域应用程序，可缩短应用程序的加载时间，并且它补充了当今可用的现有应用程序入门工作流程。 有关更多信息，请参阅以下主题： • the section called “管理应用程序组件” • the section called “AWS Resilience Hub 资源分组建议”	2024 年 8 月 1 日

AWS Resilience Hub 引入了新的评估摘要小工具	AWS Resilience Hub 推出了一个新的评估摘要小工具，该小工具使用 Amazon Bedrock 生成式 AI 功能将复杂的弹性数据转化为高度可操作的见解。这些评估摘要提取关键发现，对风险进行优先级排序，并建议提高应变能力的措施。通过关注最具影响力的元素，您可以更轻松地理解评估，这可以帮助您获得具有高影响力的信息，这些信息侧重于您的应变态势中最关键的要素。 有关更多信息，请参阅 the section called “评估摘要”。	2024 年 8 月 1 日
AWS Resilience Hub 扩展对亚马逊 DocumentDB 的支持	此 AWS Resilience Hub 策略允许您授予`Describe`权限，允许您在运行评估 AWS Lambda 时访问 Amazon DocumentDB、弹性负载平衡上的资源和配置。 有关 AWS 托管策略的更多信息，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2024 年 8 月 1 日

AWS Resilience Hub 扩展了应用程序弹性漂移检测能力	AWS Resilience Hub 通过引入一种新型的漂移检测——应用程序资源漂移，扩展了其漂移检测能力。此增强功能可检测更改，例如在应用程序的输入源中添加或删除资源。您可以启用 AWS Resilience Hub 预定评估和偏差通知服务，并在出现偏差时收到通知。最新的弹性评估可识别差异并提出补救措施，以使应用程序恢复符合您的弹性政策。 有关更多信息，请参阅以下主题： • the section called “偏差检测” • the section called “设置预定评估和偏差通知”	2024 年 5 月 8 日
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 （例如亚马逊 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 扩展对适用于 Windows 文件服务器的 Amazon FSx 的支持	AWS Resilience Hub 扩展对适用于 Windows 文件服务器的 Amazon FSx 资源的评估支持，同时评估您的应用程序的弹性。对于使用适用于 Windows 文件服务器的 Amazon FSx 的应用程序，AWS Resilience Hub 提供了一组新的弹性建议，涵盖可用区 (AZ) 和 Multi-AZ 部署、备份计划以及数据复制。AWS Resilience Hub 支持适用于 Windows 文件服务器的 Amazon FSx，包括对微软 Active Directory 的文件系统依赖关系，适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 “AWSResilienceHubAssessmentExecutionPolicy” • the section called “在应用程序组件中对资源进行分组”	2024 年 3 月 26 日
AWS Resilience Hub 提供有关弹性分数的更多信息	AWS Resilience Hub 更新了弹性评分用户体验，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 扩展对包含 Amazon Elastic Kubernetes 服务 (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，以纳入新的操作建议。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 “管理 AWS Fault Injection Service 实验”。	2023 年 11 月 9 日
AWS Resilience Hub 在应用程序级别提供更多信息	AWS Resilience Hub 在应用程序级别提供有关预计工作负载 RTO 和预计工作负载 RPO 的更多信息。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 “管理 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 在评估应用程序弹性的同时，扩展对 AWS Step Functions 资源的评估支持。 AWS Resilience Hub 分析包括状态机类型（标准或快速工作流程）在内的 AWS Step Functions 配置。此外，还 AWS Resilience Hub 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读取 AWS Step Functions 配置的特定权限 AWS Resilience Hub 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 增加了排除操作建议的能力，包括警报、标准操作程序 (SOP) 和 AWS Fault Injection Service (AWS FIS) 测试。在上运行评估时 AWS Resilience Hub，系统会向您提供预计的恢复时间以及有关如何提高所评估应用程序弹性的建议。使用排除推荐工作流程，您现在可以排除与之无关的推荐警报、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

改进的权限设计 AWS Resilience Hub	AWS Resilience Hub 引入了新的权限设计，可在配置 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

应用程序弹性偏差检测 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操作。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 “设置预定评估和偏差通知” • the section called “编辑应用程序资源”	2023 年 8 月 2 日

AWS Resilience Hub 改进了对亚马逊关系数据库服务和亚马逊 Aurora 的支持	AWS Resilience Hub 扩展了对亚马逊关系数据库服务代理、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，以提供更精确的预计工作负载恢复时间目标 (RTO)。 AWS Resilience Hub 还将提供其他措施，以在您的 AWS 环境中实施弹性最佳实践。最佳实践可能包括使用 DevOps Guru for Amazon RDS 实现性能洞察、增强监控以及在支持的数据库引擎上实现 blue/green 部署自动化。 要详细了解在评估中 AWS Resilience Hub 加入来自所有支持服务的资源所需的权限，请参阅the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 8 月 2 日

AWS Resilience Hub 扩展对亚马逊弹性区块商店快照的支持	AWS Resilience Hub 扩展了对亚马逊弹性区块商店（亚马逊 EBS）的评估支持，以识别使用直接 API 在同一亚马逊 EBS 区域内拍摄的亚马逊 EBS 快照。扩展支持是对当前使用亚马逊数据生命周期管理器（亚马逊数据生命周期管理器）或 AWS 备份的客户的支持的补充。 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（亚马逊 EC2）的支持。对于不同规模的应用程序，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： • On-demand 实例。 • 使用 AWS Backup 和备份实例 AWS 弹性灾难恢复。 • 支持使用亚马逊应用程序恢复控制器 (ARC) (ARC) 的自动扩展群组 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	添加了一项新政策，该政策允许访问其他 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 扩大了对 AWS Trusted Advisor 使用亚马逊 DynamoDB 的应用程序的支持。 AWS Trusted Advisor 与一起使用时 AWS Resilience Hub，在过去 30 天内未对应用程序进行评估时，您现在可以收到通知。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	除了目前对亚马逊简单存储服务 (Amazon S3) Cross-Region 复制 (Amazon S3 CRR) / 亚马逊S3 Same-Region 复制 (SRR)、版本控制和 AWS 备份的支持外，现在还 AWS Resilience Hub 将评估亚马逊S3的多区域接入点、亚马逊S3复制时间控制 (Amazon S3 RTC) 和 AWS 备份时间点恢复 (PITR) 配置。 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 MyApplications AWS Resource Groups添加应用程序资源。此外，客户可以直接在一个或多个区域中添加一个或多个 Amazon EKS 集群，每个集群中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、副本和 Pod 之外 ReplicationControllers，还 AWS Resilience Hub 将分析集群的整体弹性。 AWS Resilience Hub 支持无状态的亚马逊 EKS 集群工作负载。新功能在所有支持的 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 “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，现在还 AWS Resilience Hub 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 现在可以透明地显示您的应用程序源。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相关的资源的更多信息。有了这些信息，AWS Resilience Hub 可以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 “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，现在还 AWS Resilience Hub 将评估亚马逊数据生命周期管理器的亚马逊EBS快照和亚马逊EBS快速快照恢复（FSR）。 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 用户将能够查看经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，并提供状态以表明目标弹性策略（RTO 和 RPO）是否已满足。每次进行评估时，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 AWS Well-Architected 指导方针的服务。 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，并提供建议以满足该组织对应用程序的预计工作负载恢复目标（预计工作负载 RTO 和预计工作负载 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 “身份和访问管理” • the section called “在应用程序组件中对资源进行分组”	2022 年 11 月 16 日

对亚马逊应用程序恢复控制器 (ARC)（亚马逊 ARC）的额外支持	AWS Resilience Hub 现在正在评估亚马逊ARC的弹性负载平衡和亚马逊关系数据库服务（Amazon RDS），其中包括建议亚马逊ARC何时会受益。将亚马逊 ARC 评估支持扩展 AWS Resilience Hub到 A AWS uto Scaling Group (AWS ASG) 和 Amazon DynamoDB 以外。Amazon ARC 为您的应用程序提供高可用性，使您可以快速将整个应用程序故障转移到故障转移区域。 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 “身份和访问管理”	2022 年 11 月 16 日

对 AWS 备份的额外支持	AWS Resilience Hub 现在正在评估亚马逊ARC的弹性负载平衡和亚马逊关系数据库服务（Amazon RDS），其中包括建议亚马逊ARC何时会受益。将亚马逊 ARC 评估支持扩展 AWS Resilience Hub到 A AWS uto Scaling Group (AWS ASG) 和 Amazon DynamoDB 以外。Amazon ARC 为您的应用程序提供高可用性，使您可以快速将整个应用程序故障转移到故障转移区域。 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 “身份和访问管理”	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 和 AWS 备份添加到 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
介绍 AWS Resilience Hub	AWS Resilience Hub 现在可用。本指南介绍如何使用 AWS Resilience Hub 来分析基础架构、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

下一代弹性中心

下一代 Resilience Hub 是一项弹性管理服务，它使用 GenAI-powered 故障模式评估、自动依赖关系发现、弹性测试和组合弹性策略来帮助您主动评估、测试和改善 AWS 应用程序的弹性状况。

主题

- 什么是下一代弹性中心？
- 设置下一代弹性中心
- 下一代弹性中心入门
- 系统、用户旅程和服务
- 弹性政策
- 评测
- 弹性测试
- 仪表板和报告
- AWS Organizations 集成
- 迁移来源 AWS Resilience Hub
- 下一代弹性中心的安全性
- 监控下一代弹性中心
- 限额和限制
- 对下一代弹性中心进行故障排除
- API 参考
- 下一代 Resilence Hub 用户指南的文档历史记录

什么是下一代弹性中心？

下一代 Resilience Hub 是一项弹性管理服务，可帮助您定义弹性目标、对应用程序进行建模、发现依赖关系、测试弹性，并根据这些目标评估您的弹性状况。下一代 Resilience Hub 使用基于该 AWS Well-Architected 框架的 GenAI-powered 故障模式评估来识别潜在的弱点并提供切实可行的建议。AWS 推荐的弹性测试可验证您的服务如何响应符合故障边界和依赖关系的特定故障场景并从中恢复。

关键功能一览

下一代 Resilience Hub 提供以下关键功能：

- 应用程序建模 -使用与组织对应用程序的看法相匹配的层次结构对应用程序进行建模。系统代表您的业务应用程序，用户旅程描述系统内关键的最终用户路径，服务是构成支持用户旅程的 AWS 资源的组成部分。您可以定义在何处找到 AWS 资源（AWS CloudFormation 堆栈、Terraform 状态文件、资源标签或 Amazon EKS 集群），Resilence Hub 会自动发现资源并将其映射到显示资源连接方式的拓扑结构中。
- 依赖关系发现 -持续发现和映射服务的依赖关系，包括 AWS 服务、内部端点和第三方端点。
- 故障模式评估 (GenAI-powered) — 根据弹性策略和 AWS Well-Architected 最佳实践分析您的服务，以确定潜在的故障模式并提出改进建议。
- 弹性测试 — 测试您的服务以验证恢复目标是否得到满足以及依赖关系是否符合预期，例如可用区损害、区域受损和依赖关系故障。
- 弹性策略 — 可用性 SLO、灾难恢复、 Multi-Region 灾难恢复和数据恢复目标 Multi-AZ 的模块化、可组合的要求。
- AWS 组织整合 — 通过委托管理员支持和组织范围的弹性政策，对多个账户进行集中治理。

对于企业级部署，下一代 Resilience Hub 与 AWS 组织集成，通过单个委派管理员帐户为整个组织提供集中式弹性管理。无需登录个人账户，即可在组织范围内了解弹性状况和汇总仪表板。

支持的区域和可用性

下一代弹性集线器可在以下 AWS 区域版本中使用。

区域名称	区域代码
美国东部（弗吉尼亚州北部）	us-east-1
美国东部（俄亥俄州）	us-east-2
美国西部（俄勒冈州）	us-west-2
加拿大（中部）	ca-central-1
欧洲地区（爱尔兰）	eu-west-1
欧洲地区（伦敦）	eu-west-2
欧洲地区（法兰克福）	eu-central-1
欧洲地区（巴黎）	eu-west-3

区域名称	区域代码
欧洲地区（斯德哥尔摩）	eu-north-1
亚太地区（孟买）	ap-south-1
亚太地区 (新加坡)	ap-southeast-1
亚太地区（悉尼）	ap-southeast-2
亚太地区（东京）	ap-northeast-1
亚太地区 (首尔)	ap-northeast-2
南美洲（圣保罗）	sa-east-1

有关可用 AWS 区域的最新信息，请参阅《 AWS 一般参考》中的下一代 Resilience Hub 端点和配额。

定价概览

下一代 Resilience Hub 使用基于服务的定价模型。下表汇总了定价组成部分。

组件	Price
服务费（包括最多 150 个资源和每月 2 次故障模式评估）	每项服务每月 15 美元
超过 150 的额外资源以及 2 次之后的每项评估都包括在内	每次故障模式评估每项资源 0.10 美元
依赖关系发现（可选插件）	每项服务每月 10 美元
弹性测试（可选）	每分钟故障注入服务 (FIS) 0.10 美元

服务费包括每月两次针对最多 150 个资源的服务进行故障模式评估。对于超过 150 个资源的服务，每项包含的故障模式评估在超过 150 个资源的阈值时，每项资源将额外收取 0.10 美元的费用。对于两项以外的其他摊款，每项应摊款资源的费用为0.10美元，至少为50个资源。

依赖关系发现是一个可选插件，可连续自动识别您的服务调用的所有依赖关系。

弹性测试由 AWS Fault Injection Service (AWS FIS) 提供支持。对于每增加一个目标账户，您将被收取每操作分钟 0.10 美元的费用，外加每增加一个操作分钟 0.10 美元的费用。有关详细的定价信息，请参阅AWS FIS 定价。下一代 Resilience Hub 生成的弹性测试报告包含在内，无需额外付费。

有关详细的定价信息，请参阅下一代弹性中心定价。

相关服务

以下 AWS 服务集成或补充了下一代 Resilience Hub：

- AWS Fault Injection Service (AWS FIS) — 弹性测试用于 AWS FIS 向您的服务注入受控故障，以帮助您验证其运行和恢复是否如预期。有关更多信息，请参阅 弹性测试。
- AWS 应用程序恢复控制器 (ARC) — 提供准备情况检查、路由控制和区域转移功能，以补充下一代 Resilience Hub。
- AWS Well-Architected 框架 — 故障模式评估利用 Well-Architected 最佳实践来评估您的服务架构。
- AWS 组织 — 通过单个委托管理员账户的下一代 Resilience Hub 实现多账户弹性治理。
- 亚马逊 EventBridge — 使用亚马逊 EventBridge 接收来自下一代 Resilience Hub 的通知事件，以完成评估、寻找解决方案和发现依赖关系。您可以使用这些事件来构建事件驱动的自动化工作流程。

设置下一代弹性中心

在使用下一代 Resilience Hub 之前，必须完成本节中描述的设置步骤。

主题

- 先决条件
- 所需的 IAM 权限和角色
- AWS 下一代弹性中心的管理策略
- 配置 AWS 组织集成（可选）
- Multi-account 设置（没有 AWS 组织）
- Customer-managed 密钥（可选）

先决条件

在您开始之前，请确保您已拥有以下各项：

- 活跃 AWS 账户的。

- 在您的账户中创建角色和策略的 IAM 权限。
- （可选）如果您计划使用多账户监管，请配置 AWS 组织。
- （可选）AWS 通过Terraform AWS CloudFormation、资源标签或您想要评估的亚马逊弹性Kubernetes服务部署的资源。
- （可选）用于弹性测试的 IAM 执行角色。有关更多信息，请参阅 用于弹性测试的 IAM 执行角色。

所需的 IAM 权限和角色

AWS 管理的策略

您可以将 AWSResilienceHubV2AssessmentExecutionPolicy 附加得到 IAM 身份。在运行评估时，此策略向其他 AWS 服务授予只读访问权限，以进行弹性发现、评估和管理。有关此策略中包含的权限的详细信息，请参阅AWSResilienceHubV2AssessmentExecutionPolicy。

> **Note**
>
> 它用下一AWSResilienceHubV2AssessmentExecutionPolicy代的 R AWSResilienceHubAsssessmentExecutionPolicy esilience Hub 取代了之前使用的版本。

如果您使用弹性测试，还要附上AWSResilienceHubResilienceTestingPolicy托管策略。该政策向Resilience Hub授予代表您启动和管理实验所需的 AWS Fault Injection Service (AWS FIS) 权限。有关此策略中包含的权限的详细信息，请参阅AWSResilienceHubResilienceTestingPolicy。

> **Note**
>
> 如果您的账户中没有该托管策略，请创建具有相同权限的内联策略。有关政策内容，请参阅AWSResilienceHubResilienceTestingPolicy。

IAM 在评估和弹性测试中的作用

要进行评估或弹性测试，下一代 Resilience Hub 必须扮演具有所需权限的 IAM 角色。该角色发现并读取您的 AWS 资源配置，并在启用弹性测试后代表您启动和管理 AWS FIS 实验。

有两种方法可以创建或配置此角色：

- 创建新的服务角色（推荐）— 当您在下一代 Resilience Hub 控制台中创建或编辑服务时，可以在 “权限模型” 下选择 “创建新角色” 。控制台会自动使用正确的信任策略创建 IAM 角色并附加AWSResilienceHubV2AssessmentExecutionPolicy托管策略。
- 使用现有服务角色 -如果您已经配置了角色，或者您更愿意在控制台之外创建角色，请选择使用现有服务角色。然后从列表中选择角色并确保该角色具有下述所需的信任策略和权限。

手动创建角色

要手动创建角色，请打开 IAM 控制台。选择自定义信任策略并使用如下信任策略：

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

要获得权限，请附加AWSResilienceHubV2AssessmentExecutionPolicy托管策略。如果您使用弹性测试，还要附上AWSResilienceHubResilienceTestingPolicy托管策略。

IAM Service-Linked 角色

下一代 Resilience Hub 使用AWSResilienceHubServiceRolePolicy托管策略自动创建 Service-Linked 角色。

Terraform 状态文件访问权限

如果您将 Terraform 状态文件包含到下一代弹性中心服务中，请使用如下策略提供从亚马逊 S3 存储桶读取 Terraform 文件的权限：

```
{
```

```
  "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"
    }
  ]
}
```

亚马逊 EKS 权限

如果您要将亚马逊 EKS 集群纳入您的下一代 Resilience Hub 服务，请遵循以下 3 步流程，提供下一代 Resilience Hub 权限，允许其使用 Kubernetes 基于角色的访问控制 (RBAC) 读取亚马逊 EKS 集群的配置数据。

第 1 步：将以下内容应用到您的 Amazon EKS 集群

这为下一代 Resilience Hub 提供了对所有命名空间所需的 Kubernetes 资源的只读访问权限：

```
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
    - services
  verbs:
    - get
    - list
```

```
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
```

```
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

第 2 步：将 IAM 角色映射到 Kubernetes 群组

将您创建的 IAM 角色映射到 `resilience-hub-eks-access-group` Kubernetes 群组。您可以使用亚马逊 EKS 访问条目（推荐）或 `aws-auth` ConfigMap.

选项 A：使用 EKS 访问条目（推荐）

EKS 访问条目是管理集群身份验证的首选方法。您的集群必须使用`API`或`API_AND_CONFIG_MAP`身份验证模式。

```
aws eks create-access-entry \
  --cluster-name cluster-name \
  --principal-arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole \
  --type STANDARD \
  --kubernetes-groups '["resilience-hub-eks-access-group"]'
```

选项 B：使用 aws-auth ConfigMap

如果您的集群使用`CONFIG_MAP`或`API_AND_CONFIG_MAP`身份验证模式，则可以改为编辑 aws-auth ConfigMap ：

使用 eksctl：

```
eksctl create iamidentitymapping \
  --cluster cluster-name \
  --region region \
  --arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole \
  --group resilience-hub-eks-access-group \
  --username AwsResilienceHubAssessmentEKSAccessRole
```

或者手动编辑 ConfigMap：

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

mapRoles在数据部分下方添加以下内容：

```
- groups:
    - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole
  username: AwsResilienceHubAssessmentEKSAccessRole
```

第 3 步：验证

确认 RBAC 资源存在且角色映射已到位：

```
kubectl get clusterrole resilience-hub-eks-access-cluster-role
kubectl describe clusterrolebinding resilience-hub-eks-access-cluster-role-binding
```

如果使用访问条目（选项 A）：

```
aws eks describe-access-entry \
  --cluster-name cluster-name \
  --principal-arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole
```

如果使用 aws-auth ConfigMap （选项 B ）：

```
kubectl get configmap aws-auth -n kube-system -o yaml | grep -A 3 "ResilienceHubRole"
```

AWS 下一代弹性中心的管理策略

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、群组和角色分配权限。

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。建议通过定义特定于您的使用场景的 客户托管式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主体身份（用户、组和角色）。 AWS 最有可能在启动新服务或新的 API 操作可用于现有 AWS 服务时更新 AWS 托管策略。

主题

- AWSResilienceHubV2AssessmentExecutionPolicy
- AWSResilienceHubResilienceTestingPolicy
- AWSResilienceHubServiceRolePolicy
- 下一代 Resilience Hub 更新至 AWS 托管策略

AWSResilienceHubV2AssessmentExecutionPolicy

您可以将 `AWSResilienceHubV2AssessmentExecutionPolicy` 附加得到 IAM 身份。在运行评估时，此策略向其他 AWS 服务授予只读访问权限，以进行弹性发现、评估和管理。

权限详细信息

此策略授予通配符只读权限，这些权限可能在输出中包含敏感信息。

该策略包含以下权限：

- 亚马逊 CloudWatch (CloudWatch) — 为与您的 AWS 账户关联的 CloudWatch 资源提供`Describe`、`Get`、和`List`权限。

- AWS CloudFormation — 为与您的 AWS 账户关联的 AWS CloudFormation 资源提供`Describe`、`Get`和`List`权限。
- 亚马逊弹性计算云 (Amazon EC2) — 为与您的 AWS 账户关联的亚马逊 EC2 资源提供特定`Describe`权限。
- 亚马逊弹性容器服务 (亚马逊 ECS) — 为`Describe`与您的 AWS 账户关联的亚马逊 ECS 资源提供和`List`权限。
- 亚马逊弹性 Kubernetes 服务（亚马逊 EKS）— 为`Describe`与您的`List`账户关联的亚马逊 EKS 资源提供和权限。 AWS
- 亚马逊弹性容器注册表 (Amazon ECR) — 为与您的 AWS 账户关联的亚马逊 ECR 资源提供`Describe`权限。
- 亚马逊弹性文件系统 (亚马逊 EFS) — 为与您的 AWS 账户关联的亚马逊 EFS 资源提供`Describe`权限。
- 亚马逊 ElastiCache (ElastiCache) — 为与您的 AWS 账户关联的 ElastiCache 资源提供`Describe`权限。
- 弹性负载平衡-为与您的 AWS 账户关联的弹性负载平衡资源提供`Describe`权限。
- 亚马逊 DynamoDB (DynamoDB) — 为`Describe`与您的账户关联的 DynamoDB 资源提供和`List`权限。 AWS
- 亚马逊 RDS — 为与您的 AWS 账户关联的亚马逊 RDS 资源提供`Describe`权限。
- 亚马逊 DocumentDB — 为`Describe`与您的 AWS 账户关联的 Amazon DocumentDB 资源提供和`List`权限。
- AWS Lambda (Lambda) — 为与您的 AWS 账户关联的 Lambda 资源提供特定`List`权限`Get`和权限。
- AWS Step Functions — 为`Describe`与您的 AWS 账户关联的 AWS Step Functions 资源提供和`List`权限。
- IAM — 为与您的 AWS 账户关联的 IAM 资源提供特定`List`权限`Get`和权限。
- 亚马逊简单通知服务 (亚马逊 SNS) — 为`Get`与您的 AWS 账户关联的亚马逊 SNS 资源提供和`List`权限。
- 亚马逊简单队列服务 (亚马逊 SQS) — 为`Get`与您的 AWS 账户关联的亚马逊 SQS 资源提供和`List`权限。
- 亚马逊简单存储服务 (Amazon S3) — 为`Get`与您的 AWS 账户关联的 Amazon S3 资源提供和`List`权限。使用`aws:ResourceAccount`条件密钥，`AWSResilienceHubS3AccessStatement`中的 Amazon S3 权限仅限于同一账户中的资源。

- 亚马逊 Route 53 (Route 53) — 为Get与您的 AWS 账户关联的 Route 53 资源（包括 Route 53 应用程序恢复控制器资源）提供和List权限。
- 亚马逊 EC2 系统管理器 (SSM) — 为Describe与您的 AWS 账户关联的 SSM 资源提供和Get权限。
- 亚马逊 EC2 自动扩展 — 为与您的 AWS 账户关联的 Amazon EC2 Auto Scaling 资源提供Describe权限。
- AWS Backup — 为与您的 AWS 账户关联的 AWS Backup 资源提供DescribeGet、和List权限。
- AWS 弹性灾难恢复（弹性灾难恢复）-为与您的 AWS 账户关联的弹性灾难恢复资源提供Describe权限。
- AWS Fault Injection Service (AWS FIS) — 为Get与您的 AWS 账户关联的 AWS FIS 实验和实验模板提供和List权限。
- 适用于 Windows 文件服务器的亚马逊 FSx (亚马逊 FSx) — 为与您的账户关联的亚马逊 FSx 资源提供Describe权限。 AWS
- 亚马逊数据生命周期管理器-为与您的 AWS 账户关联的亚马逊数据生命周期管理器资源提供Get权限。
- AWS DataSync — 为Describe与您的 AWS 账户关联的 AWS DataSync 资源提供和List权限。
- AWS Resource Groups（资源组）-为Get与您的 AWS 账户关联的资源组资源提供和List权限。
- AWS Service Catalog（服务目录）-为Get与您的 AWS 账户关联的服务目录资源提供和List权限。
- 亚马逊 API 网关 — 为 REST API、HTTP API、使用计划和域名提供特定资源 ARN 模式的GET权限。
- 亚马逊 Kinesis — 为Describe与您的 AWS 账户关联的 Kinesis 资源提供和List权限。
- 亚马逊 Kinesis Data Firehose — 为Describe与您的List账户关联的 Kinesis Data Firehose 资源提供和权限。 AWS
- 亚马逊 EventBridge — 为Describe与您的 AWS 账户关联的 EventBridge 资源提供和List权限。
- 亚马逊 MSK — 为Describe与Get您的账户关联的亚马逊 MSK 和 MSK Connect 资源提供和List权限。 AWS
- 亚马逊 MemoryDB — 为与您的账户关联的 MemoryDB 资源提供Describe权限。 AWS
- 亚马逊 Redshift — 为与您的 AWS 账户关联的 Redshift 资源提供Describe权限。
- AWS 全球加速器-为Describe与您的 AWS 账户关联的全球加速器资源提供和List权限。
- AWS 网络防火墙-为Describe与您的 AWS 帐户关联的网络防火墙资源提供和List权限。
- AWS 盾牌 — 为Describe与您的 AWS 账户关联的 Shield 资源提供和List权限。

- AWS WAF V2 — 为Get与您的 AWS 账户关联的 WAF V2 资源提供和List权限。
- AWS 资源访问管理器-为Get与您的 AWS 账户关联的 RAM 资源提供和List权限。
- 亚马逊 VPC Lattice — 为Get与您的 AWS 账户关联的 VPC 莱迪思资源提供和List权限。
- AWS 配置-为Describe与您的 AWS 账户关联的配置资源提供和List权限。
- 亚马逊 CloudFront — 为Get与您的 AWS 账户关联的 CloudFront 资源提供和List权限。
- AWS 密钥管理器-为Describe与您的 AWS 账户关联的密钥管理器资源提供和List权限。
- AWS 目录服务-为与您的 AWS 帐户关联的目录服务资源提供Describe权限。
- 亚马逊 DSQL — 为Get与您的 AWS 账户关联的 DSQL 资源提供和List权限。
- 亚马逊 QLDB — 为Describe与您的List账户关联的 QLDB 资源提供和权限。 AWS
- AWS 证书管理器-为与您的 AWS 账户关联的 ACM 资源提供DescribeGet、和List权限。
- 应用程序自动扩展-为与您的 AWS 账户关联的应用程序自动扩展资源提供Describe权限。
- SSM 事件-为Get与您的 AWS 账户关联的 SSM 事件资源提供和List权限。
- 标签-提供查询与您的 AWS 账户关联的已标记资源的GetResources权限。

AWS 托管策略AWSResilienceHubV2AssessmentExecutionPolicy提供这些权限。附上托管策略，而不是复制策略文档，这样您的权限在 AWS 更新时就保持最新状态。要查看完整的策略文档，请参阅AWSResilienceHubV2AssessmentExecutionPolicy《 AWS 托管策略参考指南》。

AWSResilienceHubResilienceTestingPolicy

您可以将 AWSResilienceHubResilienceTestingPolicy 附加得到 IAM 身份。该政策向 Resilience Hub授予在弹性测试期间代表您启动和管理实验所需的 AWS Fault Injection Service (AWS FIS) 权限。由 Resilence Hub 发起的实验带有标签managedBy: resiliencehub。

权限详细信息

该策略包含以下权限：

- AWS Fault Injection Service (AWS FIS) — 提供创作和管理 Resilence Hub 代表您运行的实验模板和实验的权限：创建和删除实验模板、启动和停止实验、监控实验状态、列出实验目标客户资源、在创建时标记资源以及配置多账户目标。这些操作的范围仅限于带有标签的managedBy: resiliencehub资源。
- IAM — 提供iam:PassRole将测试执行角色传递iam:CreateServiceLinkedRole给并允许 AWS FIS 创建运行实验所需的服务相关角色。 AWS FIS

- AWS 应用程序恢复控制器 (ARC) 区域切换-提供List监控作为实验一部分运行的区域切换计划执行情况的Get权限。
- 亚马逊 CloudWatch (CloudWatch) — 在弹性测试期间，作为实验后工作流程的一部分，提供DescribeAlarmHistory对客户警报进行评估。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "AWSResilienceHubFISActionStatement",
      "Effect": "Allow",
      "Action": "fis:CreateExperimentTemplate",
      "Resource": "arn:aws:fis:*:*:action/*"
    },
    {
      "Sid": "AWSResilienceHubFISCreateExperimentTemplateStatement",
      "Effect": "Allow",
      "Action": "fis:CreateExperimentTemplate",
      "Resource": "arn:aws:fis:*:*:experiment-template/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISStartExperimentFromTemplateStatement",
      "Effect": "Allow",
      "Action": "fis:StartExperiment",
      "Resource": "arn:aws:fis:*:*:experiment-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISStartExperimentStatement",
      "Effect": "Allow",
      "Action": "fis:StartExperiment",
      "Resource": "arn:aws:fis:*:*:experiment/*",
      "Condition": {
```

```
        "StringEquals": {
          "aws:RequestTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISExperimentStatement",
      "Effect": "Allow",
      "Action": [
        "fis:GetExperiment",
        "fis:StopExperiment",
        "fis:ListExperimentResolvedTargets"
      ],
      "Resource": "arn:aws:fis:*:*:experiment/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISExperimentTemplateStatement",
      "Effect": "Allow",
      "Action": [
        "fis:CreateTargetAccountConfiguration",
        "fis:DeleteExperimentTemplate"
      ],
      "Resource": "arn:aws:fis:*:*:experiment-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubFISPassRoleStatement",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::*:role/*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "fis.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid": "AWSResilienceHubFISTagResourceStatement",
      "Effect": "Allow",
      "Action": "fis:TagResource",
      "Resource": [
        "arn:aws:fis:*:*:experiment-template/*",
        "arn:aws:fis:*:*:experiment/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedBy": "resiliencehub"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubRegionSwitchStatement",
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:GetPlanExecution"
      ],
      "Resource": "arn:aws:arc-region-switch::*:plan/*:*"
    },
    {
      "Sid": "AWSResilienceHubFISCreateSLRStatement",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AWSResilienceHubCloudWatchAlarmStatement",
      "Effect": "Allow",
      "Action": "cloudwatch:DescribeAlarmHistory",
      "Resource": "*"
    }
  ]
}
```

AWSResilienceHubServiceRolePolicy

AWSResilienceHubServiceRolePolicy这是一项服务相关角色 (SLR) 策略。您无法将此策略附加到您的 IAM 实体。当您启用 AWS 组织对多账户弹性管理的支持时，下一代 Resilience Hub 会自动创建此服务相关角色。这个角色信任resiliencehub.amazonaws.com服务主体。

有关 Resilience Hub 的服务相关角色的 AWS 更多信息，请参阅为 Resilience Hub 使用服务相关角色 AWS 。

权限详细信息

通过此政策，下一代弹性中心可以访问只读 AWS 组织信息，以进行多账户弹性管理。

该策略包含以下权限：

- AWS 组织-为组织资源提供Describe和List权限。这些权限可发现组织结构、识别委派管理员并验证可信访问状态。

以下 IAM 政策为下一代弹性中心提供了访问 AWS 组织资源进行多账户弹性管理所需的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSResilienceHubOrganizationsReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListDelegatedServicesForAccount",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListRoots",
                "organizations:ListTagsForResource"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

下一代 Resilience Hub 更新至 AWS 托管策略

查看自该服务开始跟踪这些变化以来下一代Resilience Hub AWS 管理策略更新的详细信息。要自动收到有关此页面更改的警报，请订阅下一代 Resilence Hub 文档历史记录页面上的 RSS 提要。

更改	描述	日期
AWSResilienceHubResilienceTestingPolicy - 新策略	AWS 为下一代 Resilience Hub 添加了一项新政策，以授予在弹性测试期间代表您启动和管理实验所需的 AWS Fault Injection Service (AWS FIS) 权限。	2026 年 7 月 31 日
AWSResilienceHubServiceRolePolicy：对现有策略的更新	下一代 Resilience Hub 向添加了只读 AWS 组织权限`AWSResilienceHubServiceRolePolicy` 。这些权限支持多账户弹性管理，包括发现组织结构、识别委派管理员和验证可信访问状态。	2026 年 7 月 7 日
AWSResilienceHubV2AssessmentExecutionPolicy：新策略	下一代 Resilience Hub 添加了一项新政策，向其他 AWS 服务授予只读访问权限，以进行弹性发现、评估和管理。	2026 年 6 月 18 日
下一代 Resilience Hub 开始追踪变化	下一代 Resilience Hub 开始跟踪其 AWS 托管策略的变化。	2026 年 6 月 18 日

配置 AWS 组织集成（可选）

如果您使用 AWS Organizations，则可以选择配置下一代 Resilience Hub，以便在整个组织中提供集中治理。以下是快速设置摘要：

1. 管理账户为启用了可信访问`resiliencehub.amazonaws.com`。
2. Service-Linked 在所有成员账户中自动创建角色 (`AWSServiceRoleForResilienceHub`)。
3. 管理账户注册委托管理员。
4. 委派管理员选择一个主区域进行数据聚合。

成员账户中的个人服务所有者仍会为其服务创建自己的调用者角色。SLR 向委派管理员提供只读的跨账户可见性。

设置主区域

如果您使用 AWS 组织，则委派管理员会选择一个汇总组织级数据的主区域。主区域是收集所有组织级摘要数据 AWS 区域 的地方，用于集中报告和仪表板。

选择主地区时，请选择一个符合以下条件的地区：

- 离您的主要运营团队很近。
- 满足您的数据驻留要求。

服务摘要数据（标识符、合规性分数、状态）从所有区域和账户复制到本地区，便于快速、集中查询。拓扑、发现和依赖关系等完整详细信息保留在其来源区域中，可按需访问。

有关详细设置说明，请参阅AWS Organizations 集成。

Multi-account 设置（没有 AWS 组织）

如果您的服务资源跨越多个 AWS 账户，并且您没有使用 AWS 组织，则除了调用者角色外，您还需要跨账户角色。

第 1 步：创建跨账户角色

在包含服务资源的每个账户中，使用以下命令创建一个角色：

- `ReadOnlyAccess`政策已附上。
- 一种信任策略，允许调用者角色代入该策略，使用`ExternalId`来防止混乱的副手攻击。为每种服务和账户组合使用唯一的`ExternalId`价值：

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

```
    "Effect": "Allow",
    "Principal": {
      "Service": "resiliencehub.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "ngrh-my-service-111122223333"
      }
    }
  }]
}
```

第 2 步：授予调用者角色代入跨账户角色的权限

向您的调用者角色添加内联策略，允许其代入跨账户角色：

```
{
  "Effect": "Allow",
  "Action": "sts:AssumeRole",
  "Resource": [
    "arn:aws:iam::111122223333:role/NGRHResourceRole",
    "arn:aws:iam::444455556666:role/NGRHResourceRole"
  ]
}
```

第 3 步：在您的服务上配置跨账户角色

创建服务时指定跨账户角色 ARN 和外部 ID：

```
aws resiliencehubv2 create-service \
  --name "my-service" \
  --regions '["us-east-1"]' \
  --permission-model '{
    "invokerRoleName": "AWSResilienceHubAssessmentRole",
```

```
    "crossAccountRoles": [
      {
        "crossAccountRoleArn": "arn:aws:iam::111122223333:role/NGRHResourceRole",
        "externalId": "ngrh-my-service-111122223333"
      },
      {
        "crossAccountRoleArn": "arn:aws:iam::444455556666:role/NGRHResourceRole",
        "externalId": "ngrh-my-service-444455556666"
      }
    ]
  }'
```

您最多可以为每个服务配置 5 个跨账户角色 ARN。

Customer-managed 密钥（可选）

下一代 Resilience Hub 支持客户管理的 AWS KMS 密钥 (CMK)，用于加密您的数据。要使用 CMK，请确保您的 IAM 策略包含以下 AWS KMS 权限：

- `kms:DescribeKey`
- `kms:GenerateDataKey`
- `kms:Encrypt`
- `kms:Decrypt`

对于定期或长期评估，还包括`kms:CreateGrant`。

无需更改调用者角色即可进行 CMK 加密。下一代 Resilence Hub 使用您的呼叫者身份进行同步操作，使用 AWS KMS 拨款进行异步操作。

下一代弹性中心入门

本教程将引导您完成使用下一代 Resilience Hub 的端到端工作流程，从创建您的第一项服务到查看故障模式调查结果。

主题

- 教程概述和先决条件
- 步骤 1：配置弹性策略
- 第 2 步：创建您的第一个系统和服务

- 第 3 步：进行首次故障模式评估
- 第 4 步：查看故障模式的调查结果和建议
- 第 5 步：启用依赖项发现（可选）
- 第 6 步：进行第一次弹性测试（可选）

教程概述和先决条件

本教程将引导您完成创建第一个系统和服务、运行故障模式评估以及查看结果的端到端工作流程。最后，您将对其中一个应用程序进行工作弹性评估。

步骤	你会做什么	估计时间
1	配置弹性策略	3 分钟
2	创建您的第一个系统和服务	5 分钟
3	进行首次故障模式评估	5—15 分钟（异步）
4	审查调查结果和建议	10 分钟
5	启用依赖项发现（可选）	5 分钟
6	进行第一次弹性测试（可选）	10 分钟

总时间：大约 40—50 分钟。

在开始本教程之前，请确保满足以下条件：

- 您有一个已部署 AWS 账户 的资源（AWS CloudFormation 堆栈、标记资源或 Amazon EKS 集群）。
- 您拥有下一代弹性中心的 IAM 服务角色。您可以在创建服务时让控制台自动创建一个，也可以事先手动创建一个。有关更多信息，请参阅 所需的 IAM 权限和角色。
- 您拥有 IAM 权限来调用下一代弹性中心 API。

步骤 1：配置弹性策略

弹性策略定义了服务的弹性目标，例如可用性 SLO 目标、恢复时间目标 (RTO) 和恢复点目标 (RPO)。在此步骤中，您将创建策略并将其应用于您的服务。

控制台：

1. 选择策略 > 创建策略。
2. 输入名称（例如，`Standard Availability`）。
3. 启用可用性 SLO 并将其设置为。`99.9%`
4. （可选）如果您的应用程序跨越区域，则启用 Multi-Region DR。
5. 选择创建。
6. 导航到您的服务并应用政策。

AWS CLI：

```
# Create the policy
aws resiliencehubv2 create-policy \
  --name "standard-availability" \
  --availability-slo '{"target": 99.9}'

# Apply the policy to your service
aws resiliencehubv2 update-service \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456" \
  --policy-arn "arn:aws:resiliencehub:us-east-1:123456789012:policy/standard-
availability:ghi789"
```

有关策略的更多信息，请参阅弹性政策。

第 2 步：创建您的第一个系统和服务

下一代弹性中心中的系统代表业务应用程序。服务代表该系统中可部署的组件。在此步骤中，您将创建第一个系统并将服务与之关联。

创建系统

控制台：

1. 打开下一代 Resilience Hub 控制台。
2. 选择 “系统” > “创建系统”。
3. 输入名称（例如`My Application`）和可选描述。
4. 选择创建。

AWS CLI：

```
aws resiliencehubv2 create-system \
  --name "my-application" \
  --description "My first application in Resilience Hub"
```

创建服务

服务代表可部署的组件。创建服务时，应将其与您的系统关联，并指定下一代 Resilience Hub 应在哪里查找您的 AWS 资源（输入源）。

控制台：

1. 选择 “服务” > “创建服务”。
2. 输入名称（例如，`api-service`）。
3. 选择您的系统。
4. 在 “权限模型” 下，执行以下任一操作：
   - 要让控制台自动创建所需角色，请选择创建新角色。
   - 如果您已有角色，请选择 “使用现有服务角色”，然后从列表中进行选择。
5. 在输入源下，添加您的 AWS CloudFormation 堆栈 ARN、资源标签或 Terraform 状态文件位置。
6. 选择创建。

AWS CLI：

```
aws resiliencehubv2 create-service \
  --name "api-service" \
  --regions '["us-east-1"]' \
  --associated-systems '[{"systemArn": "arn:aws:resiliencehub:us-
east-1:123456789012:system/my-application:abc123"}]' \
  --permission-model '{"invokerRoleName": "AWSResilienceHubAssessmentRole"}'
```

将服务与系统关联

创建系统和服务后，通过创建用户旅程将服务与系统关联起来。

控制台：

1. 选择 “系统”，然后选择您的系统名称。
2. 选择 “创建用户旅程” 。
3. 输入用户旅程的名称（例如，`checkout process`）。
4. 选择您创建的服务，将其与该用户旅程相关联。
5. 选择 “创建用户旅程” 。

第 3 步：进行首次故障模式评估

创建服务并应用策略后，您现在可以运行故障模式评估。在评估期间，下一代 Resilience Hub 会自动发现您的资源并建立拓扑，然后再分析故障模式。

控制台：

1. 导航到您的服务。
2. 选择失败模式指南，然后添加有关您的服务的所有断言。有关更多信息，请参阅 故障模式指导。
3. 选择 “运行故障模式评估” 。
4. 等待评估完成。这通常需要 5—15 分钟。

AWS CLI：

```
aws resiliencehubv2 start-failure-mode-assessment \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456"
```

要检查评估状态，请执行以下操作：

```
aws resiliencehubv2 list-failure-mode-assessments \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456"
```

评估期间会发生什么

在评估运行期间，下一代弹性中心将在后台执行以下步骤：

1. 下一代 Resilience Hub 将扮演你的调用者角色。
2. 它从你配置的输入源（标签AWS CloudFormation、Terraform、亚马逊 EKS）中读取资源。
3. 它识别父子关系（例如，Auto Scaling 组与 EC2 实例）。
4. Resilience Hub 为您的服务建立了拓扑结构。
5. 它建立了一个显示数据流和封闭的拓扑结构。
6. 多代理人工智能系统会根据您的弹性策略和 AWS Well-Architected 最佳实践分析架构中的故障模式。

拓扑生成完成后，您可以在控制台中查看结果：

- 图表视图 — 资源和连接的可视化地图。
- 表格视图 -包含元数据的所有已发现资源的列表。
- JSON 导出 — 下载完整拓扑结构以进行外部分析。

第 4 步：查看故障模式的调查结果和建议

评估完成后，查看结果以了解服务中潜在的故障模式和建议的改进措施。

控制台：

1. 导航到您的服务并选择故障模式选项卡。
2. 查看按严重程度排序的调查结果。
3. 选择任意发现以查看详细的理由和建议。

AWS CLI：

```
aws resiliencehubv2 list-failure-mode-findings \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456"
```

了解你的发现

每一项发现都告诉你：

- 故障模式是什么（例如，“Single-AZ RDS 数据库”）。
- 为什么它对您的架构很重要。
- 如何修复该问题，并提供包括成本和复杂性考虑在内的建议。
- 它与哪项政策要求有关。

采取行动

对于每一项发现，你可以：

- 原因 — 详细考虑故障模式，并解释失效模式发生的可能性和影响。
- 修复 — 如果可能性和影响需要的话，实施建议，然后重新进行评估以进行验证。
- 标记为无关紧要 -如果发现不适用于您的用例，则将其隐藏。在未来的评估中，被抑制的调查结果仍处于抑制状态。
- 优先级 -使用严重性来决定首先要解决的问题。

第 5 步：启用依赖项发现（可选）

依赖关系发现会自动识别您的 AWS 服务调用的服务、内部端点和第三方终端节点。它使用具有 35 天回顾窗口和持续轮询的 DNS 查询日志分析来确定您可能不知道的依赖关系，包括意外的跨区域调用或关键的第三方依赖关系。

依赖关系发现是一个可选的插件。要启用它，请在控制台中导航到您的服务，然后选择启用依赖项发现。启用后，下一代 Resilience Hub 将开始发现依赖关系，并将其显示在服务的依赖项选项卡上。

有关更多信息，请参阅 依赖项发现。

第 6 步：进行第一次弹性测试（可选）

弹性测试通过使用 AWS Fault Injection Service ()AWS FIS注入受控故障，帮助验证您的服务是否按预期运行和恢复。在此步骤中，您将选择测试模板，为您的服务创建测试，然后开始测试运行。

控制台

1. 导航到您的服务并选择 “测试” 选项卡。您将看到根据您的服务架构和弹性政策推荐的弹性测试。
2. 选择测试模板（例如，可用区：恢复）。选择 “查看详细信息” 以了解有关推荐测试的更多信息。

3. 选择 “编辑测试配置”，提供所有必需的参数，然后保存。这将根据模板创建您的测试——您的配置将被保存并重复使用以备将来运行。您可以随时编辑测试配置。
4. 选择 “开始测试” 以开始测试运行。
5. 监控运行情况，查看恢复目标是否已实现。

AWS CLI

```
# List the available test templates
aws resiliencehubv2 list-test-templates --region us-east-1

# Create a test for your service from a template
aws resiliencehubv2 create-test \
  --test-template-arn "arn:aws:resiliencehub:us-east-1:aws:test-template/aws-az-
recovery:rtaz001" \
  --target-identifier "arn:aws:resiliencehub:us-east-1:123456789012:service/api-
service:def456" \
  --parameters '{"availabilityZone": ["us-east-1a"]}'

# Start a test run
aws resiliencehubv2 start-test-run --test-id "test-id"

# Check the status and results of the test run
aws resiliencehubv2 get-test-run --test-run-id "test-run-id"
```

有关更多信息，请参阅 弹性测试。

系统、用户旅程和服务

应用程序建模是下一代弹性中心的基础。您可以使用与您的组织对其业务应用程序的看法相匹配的系统、用户旅程和服务层次结构来对应用程序进行建模。

主题

- 概述：系统、用户旅程和服务层次结构
- 创建和管理系统
- 创建和管理用户旅程
- 创建和管理服务
- 在服务中添加和移除资源

- 从外部注册表导入应用程序上下文
- 查看服务拓扑
- 示例：对多账户应用程序进行建模

概述：系统、用户旅程和服务层次结构

下一代 Resilience Hub 中的应用程序建模层次结构包括三个级别：

- 系统 — 代表业务应用程序（例如，电子商务平台或交易系统）的顶级容器。
- 用户旅程 — 系统内的关键业务路径（例如，“购买路径” 或 “订单发货”）。
- 服务 — 由支持用户旅程的 AWS 资源、代码和可观测性构成的构件。一项服务仅属于一个系统，但可以支持多个用户旅程。

以下示例显示了电子商务平台的层次结构：

```
System (e.g., "E-commerce Platform")
### User Journey: "Path to purchase"
#   ### Service: "Auth Service"
#   ### Service: "Checkout Service"
#   ### Service: "Payment Service"
### User Journey: "Order fulfillment"
#   ### Service: "Order Management Service"
#   ### Service: "Shipping Service"
### Shared Service: "EKS Platform Service"
    (supports multiple user journeys)
```

您可以定义在何处查找 AWS 资源（AWS CloudFormation 堆栈、Terraform 状态文件、资源标签或 Amazon EKS 集群），下一代 Resilence Hub 会自动发现它们并将其映射到显示资源连接方式的拓扑结构中。

应用程序建模的工作原理

要在下一代 Resilience Hub 中对应用程序进行建模，请执行以下步骤：

1. 创建弹性策略 -定义您的可用性、灾难恢复和数据恢复目标。请参阅the section called “弹性政策”。
2. 创建系统 -定义顶级业务应用程序。请参阅the section called “创建系统”。

3. 创建用户旅程 — 定义系统内的关键业务路径。请参阅the section called “创建和管理用户旅程”。
4. 创建服务 -定义构造块并指定资源发现的输入源。请参阅the section called “创建和管理服务”。
5. 进行评估 -开始故障模式评估以确定弹性差距。请参阅the section called “失效模式评估”。

创建和管理系统

系统代表您的组织运行的业务应用程序。大多数客户为每个主要业务应用程序创建一个系统。

创建系统

创建系统（控制台）

1. 在以下网址打开下一代 Resilience Hub 控制台https://console.aws.amazon.com/resiliencehub/v2/home。
2. 在导航窗格中，选择 “系统” 。
3. 选择 “创建系统” 。
4. 提供以下详细信息：
   - 系统名称 -输入系统的描述性名称。名称必须为 1—60 个字符，可以包含字母、数字、连字符和下划线。
   - 描述 -（可选）输入描述，以帮助您的团队确定此系统的用途。
   - Cross-account 共享 —（可选）如果您希望其他 AWS 账户服务与该系统关联，请启用此设置。
   - 加密 -（可选）选择客户管理的 AWS KMS 密钥来加密系统数据。
   - 标签 -（可选）向系统添加一个或多个标签。
5. 选择 “创建系统” 。

要创建系统 (AWS CLI)

- 运行以下命令：

```
aws resiliencehubv2 create-system \
  --name "system-name" \
  --description "system-description"
```

何时创建多个系统

在以下情况下创建单独的系统：

- 应用程序或服务由不同的团队独立运营。
- 你需要对每个应用程序进行单独的弹性姿势跟踪。

在以下情况下使用单一系统：

- 多种服务协同工作以提供商业价值。
- 您想作为一个整体评估相关服务的弹性。
- 服务共享基础设施（例如，常见的亚马逊 EKS 平台）。

列出并描述系统

查看您的系统（控制台）

1. 打开下一代 Resilience Hub 控制台。
2. 在导航窗格中，选择 “系统” 。
3. 系统列表显示您账户中的所有系统及其名称、服务数量和创建日期。
4. 要查看特定系统的详细信息，请选择系统名称。

列出系统 (AWS CLI)

- 运行以下 命令：

```
aws resiliencehubv2 list-systems

aws resiliencehubv2 get-system \
  --system-arn "arn:aws:resiliencehub:region:account-id:system/system-name:id"
```

删除系统

如果系统具有服务关联，则无法将其删除。当您使用控制台删除系统时，它会自动为您删除服务关联。使用 AWS CLI 时，必须先删除所有服务关联，然后删除系统。

删除系统（控制台）

1. 打开下一代 Resilience Hub 控制台。
2. 在导航窗格中，选择 “系统” 。
3. 选择要删除的系统。
4. 选择 Actions (操作)，然后选择 Delete (删除)。
5. 在确认对话框中，选中删除确认复选框并选择删除。

删除系统 (AWS CLI)

- 运行以下命令：

```
aws resiliencehubv2 delete-system \
  --system-arn "arn:aws:resiliencehub:region:account-id:system/system-name:id"
```

创建和管理用户旅程

用户旅程描述了系统内的关键业务路径。它们可以帮助您按业务能力组织服务，并在业务层面应用弹性策略。

创建用户旅程

创建用户旅程（控制台）

1. 打开下一代 Resilience Hub 控制台。
2. 在导航窗格中，选择系统，然后选择要向其添加用户旅程的系统。
3. 选择 “用户旅程” 选项卡。
4. 选择 “创建用户旅程” 。
5. 提供以下详细信息：
   - 名称 — 输入描述业务能力的名称（例如，“购买路径” 或 “订单发货”）。以最终用户的行为命名用户旅程，而不是按照技术组件命名。
   - 描述 -（可选）输入用户旅程的描述。
   - 关联服务 -（可选）选择支持此用户旅程的服务。您可以稍后添加服务。

6. 选择 “创建用户旅程” 。

创建用户旅程 (AWS CLI)

- 运行以下命令：

```
aws resiliencehubv2 create-user-journey \
  --system-arn "arn:aws:resiliencehub:region:account-id:system/system-name:id" \
  --name "journey-name" \
  --description "journey-description"
```

定义用户旅程的指南

- 根据业务能力而不是技术组件来命名用户旅程。
- 用户旅程应代表最终用户所做的事情（例如，“查看余额”，而不是 “数据库读取”）。
- 从您最关键的用户旅程开始，并随着时间的推移增加更多用户旅程。
- 一项服务可以属于多个用户旅程——共享平台服务通常如此。

下表显示了系统及其相应用户旅程的示例：

系统	用户旅程
E-commerce 平台	购买路径、产品发现、订单配送、退货
交易系统	执行交易、检查投资组合、转移资金
故障转移编排	管理计划、执行故障转移、运行报告

更新用户旅程

更新用户旅程（控制台）

1. 打开下一代 Resilience Hub 控制台并导航到您的系统。
2. 选择 “用户旅程” 选项卡。

3. 选择要更新的用户旅程。
4. 选择编辑。
5. 根据需要修改名称、描述或关联服务。
6. 选择保存更改。

删除用户旅程

删除用户旅程（控制台）

1. 打开下一代 Resilience Hub 控制台并导航到您的系统。
2. 选择 “用户旅程” 选项卡。
3. 选择要删除的用户旅程。
4. 选择 Delete。
5. 确认删除操作。

创建和管理服务

服务是您在下一代 Resilience Hub 中与之交互的主要实体。服务代表一个由 AWS 资源、代码和可观察性组成的可部署单元。

创建服务

创建服务（控制台）

1. 打开下一代 Resilience Hub 控制台。
2. 在导航窗格中，选择服务。
3. 选择 Create service。
4. 提供以下详细信息：

   - 服务名称 -输入服务的描述性名称（例如，`checkout-service`或`payment-service`）。
   - 描述 -（可选）输入服务的描述。
   - 弹性政策 -选择与该服务关联的弹性策略。该政策定义了您的可用性 SLO 和 RTO/RPO 目标。
   - 权限模型 — 指定下一代 Resilenity Hub 用于资源发现的 IAM 角色。请选择以下选项之一：
     - 创建新的服务角色（推荐）— 控制台自动创建具有正确信任策略的 IAM 角色并附加所需的托管策略。

- 使用现有服务角色 -从列表中选择现有的 IAM 角色。确保该角色具有所需的信任策略和权限。有关更多信息，请参阅 所需的 IAM 权限和角色。
- Cross-account 角色 -（可选）如果您的资源在其他账户中，请添加跨账户角色 ARN。

- 区域 — 选择您的服务运行所在的地区。 AWS 区域您最多可以选择 5 个区域。
- 资源发现 -提供输入源以发现服务使用的资源。the section called “向服务添加输入源”有关添加输入源的说明，请参见。
- 依赖项发现 -（可选）启用此服务的依赖项发现功能。有关依赖项发现the section called “依赖项发现”的更多信息，请参阅。
- 数据加密 -（可选）选择客户管理的 AWS KMS 密钥来加密服务数据。有关更多信息，请参阅 the section called “数据加密”。
- 标签 -（可选）为您的服务添加标签。

5. 选择 Create service。

创建服务 (AWS CLI)

- 运行以下命令：

```
aws resiliencehubv2 create-service \
  --name "service-name" \
  --regions '["region"]' \
  --permission-model '{"invokerRoleName": "role-name"}' \
  --associated-systems '[{"systemArn": "system-arn"}]'
```

下表描述了在创建服务后可以添加的可用输入源类型：

输入源	使用场景
AWS CloudFormation 堆栈	您的基础架构在中定义 AWS CloudFormation。
Terraform 状态文件	您的基础设施由 Terraform（亚马逊 S3 中的状态文件）管理。
资源标签	该服务通过匹配标签来发现资源。具有多个标签的基于标签的单一输入源只能发现与所有指定标

输入源	使用场景
	签匹配的资源。多个基于标签的输入源会发现与其中任何一个匹配的资源。
亚马逊弹性 Kubernetes 服务集群	您的服务在亚马逊 EKS 上运行。

向服务添加输入源

添加输入源（控制台）

1. 打开下一代 Resilience Hub 控制台并导航到您的服务。
2. 选择配置选项卡。
3. 在“服务资源发现”部分选择“编辑”。
4. 选择输入源类型并提供所需的配置：
   - AWS CloudFormation 堆栈 -选择一个或多个 AWS CloudFormation 堆栈。选择器将显示与您为此服务选择的区域相关的堆栈。
   - Terraform 状态文件 — 输入状态文件的 Amazon S3 URL。
   - 资源标签 -输入要匹配的标签密钥和值。
   - 亚马逊 EKS 集群 — 输入集群 ARN 并选择要包含的命名空间。
5. 选择添加。

添加输入源 (AWS CLI)

- 运行以下命令：

```
aws resiliencehubv2 create-input-source \
  --service-arn "service-arn" \
  --resource-configuration '{"cfnStackArn": "stack-arn"}'
```

服务投放：相同账户与不同账户

与系统相同的帐户（简单）：系统和服务相同 AWS 账户。单个调用者角色涵盖了所有内容。这种方法最适合小型团队和单账户工作负载。

账户与系统（企业）不同：系统位于中央账户中，服务位于分支账户中。这种方法需要跨账户角色或 AWS 组织。它最适合拥有分布式所有权的大型组织。

服务功能

服务功能是服务拓扑的技术子集，代表服务内的特定工作流程。

例如，身份验证服务可能有两个服务功能：

- SSO 登录 — 涉及身份提供商、会话存储和令牌服务。
- 注册 — 涉及用户数据库、电子邮件服务和验证流程。

服务功能可帮助您了解哪些资源参与单个服务中的哪些工作流程。服务功能由下一代弹性中心在评估期间确定。

查看服务事件日志

服务事件日志按时间顺序提供服务发生的所有事件的历史记录。您可以使用事件日志来跟踪更改、解决问题和审计活动。

查看服务事件日志（控制台）

1. 导航到您的服务。
2. 选择 “操作” 按钮。
3. 选择 “查看事件日志” 。

您可以按事件类型和时间范围筛选事件。记录了以下事件类型：

- 断言已创建 -断言已添加到服务中。
- 断言已删除 -断言已从服务中删除。
- 断言已更新 -修改了现有断言。
- 可实现性已更新 -政策组成部分的可实现性状态已更改。

- 服务已创建 -服务已创建。
- 服务已删除 -服务已删除。
- 已创建函数 -已创建服务函数。
- 功能已删除 -服务功能已删除。
- 已添加功能资源 -资源已添加到服务功能。
- 移除函数资源 -资源已从服务功能中移除。
- 功能已更新 -服务功能已更新。
- 输入源已更新 -服务的输入源已修改。
- 相关政策 -与服务相关的弹性政策。
- 政策取消关联 -已从服务中移除弹性策略。
- 关联资源 -发现了新资源并与该服务相关联。
- 资源取消关联 -资源已从服务中移除。
- 系统关联 -该服务与系统关联。
- 系统取消关联 -该服务已从系统中删除。
- 工作流程已更新 -工作流程配置已更新。

每个事件条目都显示时间戳、事件类型和更改内容摘要。选择 “显示详细信息” 以查看有关特定事件的更多信息。

在服务中添加和移除资源

资源是从您配置的输入源中自动发现的。您无需手动添加单个资源。下一代 Resilience Hub 会从 AWS CloudFormation 堆栈、Terraform 状态文件、亚马逊 EKS 集群和资源标签中发现资源。

查看已发现的资源

查看资源（控制台）

1. 打开下一代 Resilience Hub 控制台并导航到您的服务。
2. 选择服务拓扑。
3. 资源图和资源列表显示所有已发现的资源及其类型、区域和相关的服务功能。
4. 使用筛选器按地区或服务功能缩小范围。

列出资源 (AWS CLI)

- 运行以下命令：

```
aws resiliencehubv2 list-resources \
  --service-arn "service-arn"
```

要按地区筛选，请执行以下操作：

```
aws resiliencehubv2 list-resources \
  --service-arn "service-arn" \
  --aws-region "region"
```

更新输入源

要更改下一代 Resilience Hub 寻找资源的位置，请在服务上添加或删除输入源。the section called “向服务添加输入源”有关添加输入源的说明，请参见。

移除输入源（控制台）

1. 打开下一代 Resilience Hub 控制台并导航到您的服务。
2. 选择配置选项卡。
3. 选择编辑。
4. 移除现有的输入源选项。
5. 选择保存更改。

移除输入源 (AWS CLI)

- 运行以下命令：

```
aws resiliencehubv2 delete-input-source \
  --service-arn "service-arn" \
  --input-source-id "input-source-id"
```

从外部注册表导入应用程序上下文

您可以从外部注册表（例如设计文档）导入应用程序上下文，以便在下一代 Resilience Hub 中丰富您的应用程序模型。导入的上下文使用资源配置中未捕获的业务元数据对 AWS 资源拓扑进行了补充。

导入设计文档

设计文档提供了下一代 Resilience Hub 在故障模式评估期间使用的额外架构背景。您可以上传存储在 Amazon S3 中的设计文档作为服务的输入源。

导入设计文档（控制台）

1. 打开下一代 Resilience Hub 控制台并导航到您的服务。
2. 选择评估选项卡。
3. 选择失效模式指南。
4. 从 “架构设计文件” 中选择 “添加更多”。
5. 输入您的设计文档的 Amazon S3 网址。
6. 选择 “保存设计文件” 。

要导入设计文档 (AWS CLI)

- 运行以下命令：

```
aws resiliencehubv2 create-input-source \
  --service-arn "service-arn" \
  --resource-configuration '{"designFileS3Url": "s3://bucket/path/to/design-doc.pdf"}'
```

支持的设计文档格式包括 PDF、Markdown 和纯文本文件。AI 评估引擎使用这些文档来了解您的预期架构，并确定设计意图与实际实施之间的差距。

查看服务拓扑

下一代 Resilience Hub 控制台提供可视化画布视图，显示您的服务层次结构，包括资源拓扑和服务功能。

查看服务拓扑

1. 打开下一代 Resilience Hub 控制台并导航到您的服务。
2. 选择服务拓扑。
3. 拓扑视图显示您发现的资源如何相互连接。资源按服务功能分组，显示代表依赖关系的边缘。
4. 选择资源节点以查看其详细信息，包括资源类型、ARN、区域和账户。

示例：对多账户应用程序进行建模

此示例说明如何在下一代 Resilience Hub 中对一个拥有 10 个账户的 30 项服务的大型电子商务平台进行建模。

对多账户应用程序进行建模

1. 在中央账户中创建系统。

   首先，创建一个代表整个电子商务平台的单一系统。在您的中央治理账户中创建系统并启用跨账户共享：

   ```
   aws resiliencehubv2 create-system \
     --name "acme-ecommerce" \
     --description "Acme Corp e-commerce platform" \
     --sharing-enabled
   ```

2. 在他们各自的账户中创建服务。

   每个团队在自己的账户中创建自己的服务，参考中央系统 ARN：

   ```
   # In account A (auth team)
   aws resiliencehubv2 create-service \
     --name "auth-service" \
     --regions '["us-east-1", "us-west-2"]' \
   ```

```
  --permission-model '{"invokerRoleName": "AWSResilienceHubAssessmentRole"}' \
  --associated-systems '[{"systemArn": "arn:aws:resiliencehub:us-
east-1:111111111111:system/acme-ecommerce:abc123"}]'

# In account B (checkout team)
aws resiliencehubv2 create-service \
  --name "checkout-service" \
  --regions '["us-east-1", "us-west-2"]' \
  --permission-model '{"invokerRoleName": "AWSResilienceHubAssessmentRole"}' \
  --associated-systems '[{"systemArn": "arn:aws:resiliencehub:us-
east-1:111111111111:system/acme-ecommerce:abc123"}]'
```

3. 向每项服务添加输入源。

   每个团队都会添加他们的资源发现配置：

```
# Auth team adds their CloudFormation stack
aws resiliencehubv2 create-input-source \
  --service-arn "arn:aws:resiliencehub:us-east-1:222222222222:service/auth-
service:def456" \
  --resource-configuration '{"cfnStackArn": "arn:aws:cloudformation:us-
east-1:222222222222:stack/auth-prod/..."}'

# Checkout team adds their EKS cluster
aws resiliencehubv2 create-input-source \
  --service-arn "arn:aws:resiliencehub:us-east-1:333333333333:service/checkout-
service:ghi789" \
  --resource-configuration '{"eks": {"clusterArn": "arn:aws:eks:us-
east-1:333333333333:cluster/checkout-cluster", "namespaces": ["checkout"]}}'
```

4. 定义用户旅程。

   在按业务能力对服务进行分组的中央账户中创建用户旅程：

```
aws resiliencehubv2 create-user-journey \
  --system-arn "arn:aws:resiliencehub:us-east-1:111111111111:system/acme-
ecommerce:abc123" \
  --name "Path to purchase" \
  --description "Customer browses, adds to cart, and completes checkout"
```

5. 应用弹性政策。

   创建策略并将其与服务关联：

```
# Create a policy
aws resiliencehubv2 create-policy \
  --name "mission-critical" \
  --availability-slo '{"target": 99.99}' \
  --multi-az '{"rtoInMinutes": 5, "rpoInMinutes": 1, "disasterRecoveryApproach":
 "ACTIVE_ACTIVE"}' \
  --multi-region '{"rtoInMinutes": 30, "rpoInMinutes": 5,
 "disasterRecoveryApproach": "WARM_STANDBY"}'

# Associate with a service
aws resiliencehubv2 update-service \
  --service-arn "arn:aws:resiliencehub:us-east-1:333333333333:service/checkout-
service:ghi789" \
  --policy-arn "arn:aws:resiliencehub:us-east-1:111111111111:policy/mission-
critical:xyz"
```

6. 进行评估。

   开始对每项服务进行故障模式评估，以确定弹性差距：

```
aws resiliencehubv2 start-failure-mode-assessment \
  --service-arn "arn:aws:resiliencehub:us-east-1:333333333333:service/checkout-
service:ghi789"
```

可以逐步添加服务——从最关键的服务开始，然后随着时间的推移增加更多服务。控制台中的系统级视图在单个画布中显示了跨账户的所有服务。

弹性政策

将您的组织复原力要求与弹性政策相匹配。弹性策略通过模块化、可组合的要求来定义您的弹性预期。您可以通过选择对您的应用程序至关重要的要求来构建策略，而不是选择单一的严格策略类型。

主题

- 了解弹性策略
- 策略组件
- 创建弹性策略
- 在用户旅程和服务级别应用策略
- 策略继承和多级评估
- 管理和更新政策

了解弹性策略

弹性策略定义了应用程序的弹性要求。每项策略都指定了下一代 Resilience Hub 在故障模式评估期间评估的目标，以确定您的应用程序是否符合您的弹性目标。

不同的利益相关者关心韧性的不同方面：

- 中央 SRE 团队专注于灾难恢复 (RTO/RPO) 和可用性目标。
- 服务团队专注于运营性能（延迟、错误率、吞吐量）。
- 合规团队专注于数据保护（数据持久性的 RPO）。

模块化策略允许每个利益相关者独立定义其需求，然后将其应用于应用程序层次结构的相应级别。

策略组件

策略包括以下组件：

可用性服务级别目标 (SLO)

为与此策略关联的服务定义目标 SLO。

Multi-Region 灾难恢复

为与此策略相关的服务定义多区域方法、目标恢复时间目标 (RTO) 和恢复点目标 (RPO)。

Multi-AZ 灾难恢复

为与此策略相关的服务定义多可用区方法、目标恢复时间目标 (RTO) 和恢复点目标 (RPO)。

数据恢复目标

定义与此策略关联的 data/storage 服务的备份间隔时间。

创建弹性策略

您可以通过下一代 Resilience Hub 控制台或 AWS CLI 创建弹性策略。

控制台：

1. 导航到弹性中心 > 策略。
2. 选择创建策略。
3. 输入策略名称和描述。
4. 选择您需要的组件：
   - 切换 Multi-Region DR 并进行设置 RTO/RPO。
   - 切换可用性 SLO 并设置目标百分比。
   - 切换数据恢复目标并设置两次备份之间的时间。
5. 选择创建。

AWS CLI：

```
aws resiliencehubv2 create-policy \
  --name "Critical Service Policy" \
  --multi-region '{"rtoInMinutes": 15, "rpoInMinutes": 5, "disasterRecoveryApproach":
 "WARM_STANDBY"}' \
  --availability-slo '{"target": 99.99}'
```

在用户旅程和服务级别应用策略

策略可以在应用程序层次结构的两个级别上应用：

级别	如何申请	通常谁拥有它
用户旅程	应用于系统内的用户旅程	中央 SRE 团队
服务	直接应用于服务实体	服务团队

要将策略应用于用户旅程，请使用以下命令。该用户旅程中的所有服务都将根据以下政策进行评估：

```
aws resiliencehubv2 update-user-journey \
  --system-arn "arn:aws:resiliencehub:region:account-id:system/system-name:id" \
  --user-journey-id "user-journey-id" \
  --policy-arn "arn:aws:resiliencehub:us-east-1:123456789012:policy/critical-dr:abc123"
```

要将策略直接应用于服务，请使用以下命令：

```
aws resiliencehubv2 update-service \
  --service-arn "arn:aws:resiliencehub:..." \
  --policy-arn "arn:aws:resiliencehub:us-east-1:123456789012:policy/high-
performance:def456"
```

策略继承和多级评估

根据适用于该服务的所有策略对服务进行评估：

- 它是直接分配的策略（如果有）。
- 从其所属的用户旅程中继承的策略。

这样可以将关注点分开：

- Central SRE 团队在用户旅程级别设置灾难恢复策略以进行治理。
- 服务团队根据运营要求在服务级别制定绩效政策。
- 这两项策略同时适用于用户旅程中的服务。

例如：

```
User Journey: "Path to Trade"
  Policy: "Trading Platform DR Policy" (Multi-Region, RTO 15 min, RPO 5 min)
  ### Service: "Order Execution"
        Policy: "Order Execution Performance Policy" (Availability 99.99%, Error <
 0.1%, p99 < 50ms)
```

“订单执行” 服务是根据这两个策略进行评估的。它必须满足用户旅程策略中的灾难恢复要求及其特定于服务的策略中的性能要求。

冲突解决

当多个策略包含对同一组件的相互冲突的要求时，下一代 Resilience Hub 会自动应用更严格的值。以下示例显示如何解决冲突的 RTO 值：

来源	组件	值
用户旅程政策	RTO	30 分钟
服务政策	RTO	15 分钟
应用值	RTO	15 分钟（更严格）

管理和更新政策

您可以从下一代 Resilience Hub 控制台或 AWS CLI 中列出、更新和删除弹性策略。

要列出您账户中的所有政策，请执行以下操作：

```
aws resiliencehubv2 list-policies
```

要更新政策，请执行以下操作：

```
aws resiliencehubv2 update-policy \
  --policy-arn "arn:aws:resiliencehub:..." \
  --availability-slo '{"target": 99.99}'
```

对策略的更改将在使用该策略的所有服务的下一次故障模式评估时生效。

您无法删除当前适用于服务或用户旅程的政策。先移除所有关联。

评测

下一代 Resilience Hub 提供了两种互补的评估功能：用于发现和分类服务依赖关系的自动依赖关系评估，以及通过 GenAI-powered 分析识别潜在弹性弱点的故障模式评估。

主题

- 依赖项发现
- 失效模式评估

依赖项发现

下一代 Resilience Hub 中的依赖关系发现可自动识别您的 AWS 服务所依赖的所有服务、内部端点和第三方端点，并评估其位置和频率。它使用 DNS 查询日志分析来显示您可能不知道的依赖关系，包括意外的跨区域调用、关键的第三方依赖关系以及不经常访问的服务，这些服务可能会在事件期间导致故障。

主题

- 依赖关系发现的工作原理
- 依赖关系发现的先决条件
- 为服务启用依赖关系发现
- 监控发现状态
- 查看已发现的依赖关系
- 将依赖关系分为硬依赖关系或软依赖关系
- 覆盖范围和已知限制
- 依赖关系发现疑难解答
- 定价

依赖关系发现的工作原理

依赖关系发现会分析 Route 53 DNS 解析器查询日志，以识别您的服务的计算资源解析的每个域名。这无需任何代理、代码更改或插桩即可显示完整的外部依赖关系。

功能	Detail
回顾窗口	35 天的 DNS 历史查询数据
持续监控	按小时汇总的持续发现
支持的依赖关系类型	AWS 服务、内部端点、第三方终端节点
属性	依赖关系归因于服务中的特定计算资源
设置	无需代理或更改代码 — 只需几分钟即可启用

支持的依赖关系类型

依赖关系发现可识别以下类型的依赖关系：

- AWS 服务终端节点 — 亚马逊 S3、亚马逊 DynamoDB、SQS 以及您的应用程序调用的 AWS 其他服务。
- 内部终端节点 — 您的 VPC 或组织内的服务。
- Third-party 端点 — 外部服务 LaunchDarkly，例如 Stripe 或 Datadog。
- Cross-region cal ls — 解析到其他 AWS 区域终端节点的依赖关系。

每个发现的依赖项都按类型分类：

Type	说明	示例
AWS 服务	AWS 服务端点	亚马逊 S3、亚马逊 DynamoDB、SQS
Third-party	外部 AWS 和您的组织中的服务	LaunchDarkly、Stripe、Datadog
Internal	组织内部的一项服务	内部微服务、共享 API

依赖关系发现与可观测性工具有何不同

依赖关系发现侧重于弹性验证，而不是操作可观察性：

能力	可观测性工具 (X-Ray, CloudWatch)	下一代弹性中心依赖关系发现
设置	需要 SDK 工具或代理	无需代理或代码更改 — 无需代理
Focus	性能监控、延迟调试	弹性验证、故障测试
Discovery	被动 — 在事故期间发现故障	主动 — 在事故发生之前发现依赖关系
分类	没有临界度分类	Hard/soft 分类
价值实现时间	数天或数周的仪器	启用需要几分钟

依赖关系发现的先决条件

在启用依赖关系发现之前，请确保满足以下要求：

- 您的服务必须具有可通过 Route 53 解析器进行 DNS 查询的计算资源（亚马逊弹性计算云实例、亚马逊弹性容器服务任务、亚马逊弹性 Kubernetes Service pod 或 VPC 绑定的 Lambda 函数）。
- 计算资源必须位于配置为使用 Route 53 DNS 解析器的 VPC 中。
- 下一代弹性中心可以发现亚马逊弹性计算云实例（首选）或亚马逊 VPC（后备）。这可以通过在控制台中查看服务拓扑来验证。
- 除了标准调用者角色之外，不需要其他 IAM 权限——依赖关系发现使用下一代 Resilience Hub 自己的服务凭证来访问 DNS 查询数据。

为服务启用依赖关系发现

您可以从控制台或使用 AWS CLI 启用依赖关系发现。

为单个服务启用依赖关系发现（控制台）

在控制台中导航到您的服务，然后选择 “评估” 选项卡。然后选择 “启用依赖关系发现”。

为单个服务启用依赖关系发现 (CLI)

```
aws resiliencehubv2 update-service \
```

```
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/checkout:abc123"
\
  --dependency-discovery "ENABLED"
```

启用依赖关系发现后，下一代 Resilience Hub 将执行以下步骤：

1. 查询服务计算资源的 35 天历史 DNS 数据。
2. 识别、删除重复数据并将依赖关系归因于您的服务。
3. 继续每小时监控一次，以检测新的依赖关系并更新现有依赖关系。
4. 在控制台的 “评估” 选项卡下显示您的服务结果。

监控发现状态

启用依赖关系发现后，`GetService`和 `ListServices` API 操作返回的`DependencyDiscoveryConfig`对象将包含一些字段，这些字段指示是否已找到符合条件的资源以及依赖关系分析是否仍在进行中。

下表描述了指示依赖关系发现当前状态的字段。

字段	Type	说明
`status`	字符串	依赖关系发现的当前状态：`INITIALIZING` `ENABLED`、或`DISABLED`。
`eligibleResourceCount`	整数	符合依赖关系发现条件的计算资源数量。该值`null`直到资源发现过程完成其第一次运行为止，并且在每次后续运行时都会更新。
`message`	字符串	描述当前发现状态的消息。`null`当发现完成且依赖关系已准备好查看时，该值即为该值。

该`message`字段根据状态和符合条件的资源的数量提供有关当前发现状态的背景信息。下表显示了可能的消息。

Status	符合条件的资源数量	Message
`INITIALIZING`	暂不可用	“发现资源”

Status	符合条件的资源数量	Message
INITIALIZING	0	“未发现符合条件的资源”
INITIALIZING	1 或更多	“发现依赖关系”
ENABLED	0	“未发现符合条件的资源”
ENABLED	1 或更多	无。依赖关系已准备就绪，可供查看。
DISABLED	Any	“启用依赖关系发现以显示依赖关系。”

以下示例说明如何使用 AWS CLI 检查发现状态。

```
aws resiliencehubv2 get-service \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/checkout:abc123"
```

响应包括dependencyDiscovery对象：

```
{
  "service": {
    ...
    "dependencyDiscovery": {
      "status": "INITIALIZING",
      "updatedAt": "2026-06-30T10:00:00Z",
      "eligibleResourceCount": 5,
      "message": "Discovering dependencies"
    }
  }
}
```

当message字段status处于null和为状态时ENABLED，依赖关系发现即告完成，结果可通过该ListDependencies操作获得。

> **Note**
>
> 如果发现完成后eligibleResourceCount为 0，请确保您的服务的计算资源满足中描述的先决条件依赖关系发现的先决条件。

查看已发现的依赖关系

启用依赖关系发现后，您可以查看包含以下列的已发现依赖关系表：

列	说明
依赖项名称	已识别的名称或域名（例如 “” 或 LaunchDarkly “api.stripe.com”）
Type	AWS 服务、第三方或内部
位置	依赖项的托管位置（例如 us-ea AWS st-1、Azure us-central 或 RFC1918）
严重性	硬性还是软性-用户分配的分类
查询频率	一段时间内的查询量可视化
第一次看见	首次发现依赖关系时
最后一次露面	对此依赖项的最新查询

依赖关系时间表

依赖关系时间轴显示了首次发现每个依赖关系的时间及其随时间变化的活动。选择任何依赖项以查看底层域名和目标 IP 地址。过去 35 天的使用频率可用，显示为单日窗口的每小时详细信息或每周窗口的每日详细信息。

计算资源归因

下一代弹性中心将发现的依赖关系归因于对这些依赖项进行 DNS 查询的特定计算资源（例如 Amazon EC2 实例、Lambda 函数或容器）。您可以按服务（在系统级别查看时）、严重程度（硬性、软性或未分类）、类型（AWS 服务、第三方或内部）或位置（AWS第三方或内部）筛选依赖关系列表。

将依赖关系分为硬依赖关系或软依赖关系

查看发现的依赖关系后，对每个依赖项进行分类以表明其对故障的影响：

```
aws resiliencehubv2 update-dependency \
  --service-arn "arn:aws:resiliencehub:..." \
  --dependency-id "dependency-id" \
```

```
  --criticality "HARD" \
  --comment "Payment processing fails completely without Stripe"
```

使用以下准则对依赖关系进行分类：

分类为	时间	示例
硬性	如果此依赖项不可用，您的服务将完全失败	主数据库、支付网关、身份验证服务
软性	您的服务已降级，但在没有这种依赖关系的情况下继续运行	分析 API、功能标志、推荐引擎

覆盖范围和已知限制

依赖关系发现涵盖通过您的 VPC 中的 Route 53 解析器进行的所有 DNS 查询，包括 IPv4 和 IPv6 查询，以及来自亚马逊 EC2、亚马逊 ECS、亚马逊 EKS 和 Lambda VPC-connected 的查询。以下已知限制适用：

限制	影响	解决办法
Non-VPC Lambda	不包括没有 VPC 连接的 Lambda 函数	将 Lambda 函数连接到 VPC
直接 IP 连接	未发现由 IP 地址（不是 DNS）建立的连接	没有解决方法
不常见的依赖关系	初始发现时可能会错过每小时调用次数少于一次的依赖关系	35 天回顾最能捕捉到；非常罕见的电话可能不会出现
Kubernetes 共享租约	Multi-tenant Amazon EKS 集群可能会将依赖关系归因于错误的服务	验证计算资源归因是否正确地将资源映射到服务

依赖关系发现疑难解答

如果依赖关系发现未返回预期结果，请查看以下常见问题：

- D@@ iscovery 未返回 EC2 实例的预期依赖关系 — 验证依赖项使用 DNS 解析（不是直接 IP），确认计算资源位于带有 Route 53 解析器的 VPC 中，并检查依赖项是否在 35 天回顾窗口内被调用。
- 发现未返回 ECS Fargate 的预期依赖关系 — 验证服务拓扑是否包含 ECS Fargate 服务的 VPC。
- 发现未返回 Lambda 函数的预期依赖关系 — 验证 Lambda 函数是否为 VPC-connected，并且服务拓扑是否包含 VPC。
- 意外的跨区域依赖关系 — Cross-region 控制台中会自动标记依赖关系。常见原因包括应用程序代码中的硬编码区域终端节点、为特定区域配置的 AWS SDK 客户端，以及第三方服务路由到非本地终端节点。
- 出现错误服务的依赖关系 — 共享 VPC 或 Amazon EKS 集群通常会出现这种情况。验证计算资源归因是否正确地将资源映射到服务。

有关其它故障排除指南，请参阅对下一代弹性中心进行故障排除。

定价

依赖关系发现是一个可选的附加组件：

组件	Price
依赖项发现	每项服务每月 10 美元

这样可以持续、自动地识别所有依赖关系，并在 35 天内进行回顾。

失效模式评估

下一代 Resilience Hub 中的故障模式评估使用 GenAI-powered 分析来识别服务中的潜在故障模式并提供切实可行的建议。评估根据您定义的弹性策略、 AWS Well-Architected 最佳实践和 AWS 弹性分析框架评估您的架构。

主题

- 失效模式评估的工作原理
- 在服务级别上运行故障模式评估
- 查看失效模式的发现结果和建议
- 评估历史和趋势

- 定价

失效模式评估的工作原理

当您运行故障模式评估时，下一代 Resilience Hub 将执行以下步骤：

1. 读取当前资源状态 -从您的 AWS 账户刷新服务的资源配置。
2. 分析拓扑 — 多代理人工智能系统检查您的资源如何连接和交互。
3. 使用弹性分析框架对照策略进行评估 -将您的架构与弹性策略进行比较。它首先进行评估，以确定政策组成部分是否可以实现。
4. 应用 AWS Well-Architected 最佳实践 -检查常见的弹性反模式。
5. 生成调查结果 — 通过严重程度、推理和建议来确定故障模式，并将结果映射到您的弹性策略。

评估引擎使用专业的人工智能代理，将 AWS Well-Architected 框架可靠性最佳实践和 AWS 弹性分析框架应用于您的特定架构。代理商分析弹性的不同方面：

- 可用性 — 单点故障、可用区分布和冗余。
- 灾难恢复 — Cross-region 功能、复制和故障转移就绪情况。
- 依赖关系弹性 — 依赖关系故障对服务的影响。
- 可观测性 — 监控可能延迟故障检测的漏洞。

故障模式评估不会消耗所有可用资源。相反，它评估被称为评估资源的资源子集。

评估资源：在弹性评估期间直接评估的顶级基础设施或服务组件。评估资源的配置是否对服务的可用性、可恢复性或容错性产生有意义的影响。超出此范围的资源不会对评估产生任何影响，也不会出现在资源清单中。

与复原力政策的关系

故障模式评估根据弹性策略中定义的目标评估您的应用程序。每项发现都与特定的政策要求相吻合，向您准确显示哪些弹性目标面临风险。例如：

```
Finding: "RDS database is not configured for Multi-AZ"
  -> Policy requirement: Multi-Region DR (RTO 15 min)
  -> Impact: Regional failover would require manual database restoration,
     exceeding the 15-minute RTO target
```

```
Finding: "No health check configured on ALB target group"
  -> Policy requirement: Availability SLO (99.99%)
  -> Impact: Unhealthy instances continue receiving traffic,
     degrading availability below target
```

故障模式指导

故障模式指导允许您引导代理拨号进入故障模式分析。

断言

断言是关于您的应用程序的陈述，为故障模式评估提供上下文。它们可以帮助生成式 AI 代理了解仅从资源配置中看不到的架构的各个方面。

断言可以是：

- User-created— 在进行评估之前，您可以添加断言。示例包括 “数据丢失不可接受”、“流量峰值是可以预测的” 或 “典型流量为 1,000 TPS，峰值达到 10,000 TPS”。
- System-generated— 评估引擎在分析期间生成断言，您可以查看、确认或调整这些断言。

断言被分类并用作杠杆点。通过确认或调整断言，您可以将评估引向更相关的调查结果。例如，如果评估假设您的应用程序必须处理 100 TPS，但实际上需要处理 10,000 TPS 的峰值，则调整该断言会改变您收到的调查结果。

服务设计文件

您可以上传包含技术设计详细信息的设计文件，这些文件将提供给 AI 代理进行故障模式分析。

在服务级别上运行故障模式评估

您可以从控制台或使用 AWS CLI 运行故障模式评估。评估是异步运行的。典型的完成时间为 5 到 15 分钟，具体取决于服务的复杂性。

先决条件

- 必须配置和访问服务的调用者角色。有关更多信息，请参阅 所需的 IAM 权限和角色。
- 该服务必须具有有效的已发现拓扑结构以及至少两个资源之间的数据流关系。有关更多信息，请参阅最低拓扑要求。
- 至少应适用一项抗灾政策。没有政策的评估仍在进行，但得出的有针对性的结果较少。

最低拓扑要求

要运行故障模式评估，您的服务必须具有至少两个资源之间的数据流关系的拓扑。

故障模式评估通过检查资源之间的关系来分析故障如何在架构中传播。如果没有连接至少两个资源的数据流关系，就没有数据流可供分析。评估无法得出有意义的结果。

有效的拓扑（可以进行评估）

通过数据流关系连接至少两个资源的任何拓扑都是有效的。例如：

- 应用程序负载均衡器将流量路由到 Amazon ECS 集群。
- 一个从 DynamoDB 表中读取的 Lambda 函数。
- 向 Lambda 函数提供消息的 Amazon SQS 队列。

拓扑无效（无法进行评估）

只有隔离资源且它们之间没有数据流关系的拓扑是无效的。例如，发现单个 Amazon S3 存储桶或多个未连接的 Amazon EC2 实例的服务没有可供评估分析的数据流。

开始故障模式评估（控制台）

1. 导航到您的服务。
2. 选择失败模式指南，然后添加有关您的服务的所有断言。有关更多信息，请参阅 故障模式指导。
3. 选择 “运行故障模式评估” 。
4. 等待评估完成（通常 5 到 15 分钟）。

开始故障模式评估 (CLI)

```
aws resiliencehubv2 start-failure-mode-assessment \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/checkout:abc123"
```

检查评估状态

```
aws resiliencehubv2 list-failure-mode-assessments \
  --service-arn "arn:aws:resiliencehub:..."
```

状态值的进度如下所示：PENDING、然后IN_PROGRESS、然后SUCCESS或FAILED。

在评估期间，下一代弹性中心在后台进行资源发现：

1. 下一代 Resilenision Hub 将扮演你的调用者角色。
2. 从您配置的输入源（标签CloudFormation、Terraform 或 Amazon EKS）读取资源。
3. 识别父子关系（例如，Auto Scaling 组与 Amazon EC2 实例）。
4. Resilience Hub 为您的服务建立了拓扑结构。
5. 构建显示数据流和封闭的拓扑。

拓扑完成后，可以在控制台中查看：

- 图表视图 — 资源和连接的可视化地图。
- 表格视图 -包含元数据的所有已发现资源的列表。
- JSON 导出 — 下载完整拓扑结构以进行外部分析。

查看失效模式的发现结果和建议

评估完成后，查看调查结果和建议：

查看调查结果（控制台）

1. 导航到您的服务并选择 “评估” 选项卡。
2. 查看按严重程度排序的调查结果。
3. 选择任意发现以查看详细的理由和建议。

列出调查结果 (CLI)

```
aws resiliencehubv2 list-failure-mode-findings \
  --service-arn "arn:aws:resiliencehub:..."
```

每项发现都包含以下信息：

字段	说明	示例
正在寻找名字	失效模式的简要描述	“Single-AZ 亚马逊关系数据库服务数据库造成了关键的单点故障”
说明	问题的详细解释	解释为什么这是一种风险的段落

字段	说明	示例
推理	为什么这对您的特定架构很重要	Architecture-specific 发现的背景
严重性	影响等级	高、中、低
故障类别	失败类型	命运共享、负载过大、延迟过长、配置错误和错误、单点故障
策略组件	这与哪些政策要求有关	Multi-AZ 灾难恢复
建议	建议的缓解措施	参见下面的建议表

每项建议都包括缓解、可观测性和测试建议：

- 缓解措施 — 为解决故障模式而更改基础架构或配置。
- 可观察性 — 监控或提醒改进以检测故障模式。
- 测试 — 一项旨在验证缓解措施是否按预期起作用的测试。

管理调查结果

对于每项发现，您可以详细推理故障模式，实施建议的修复方法，如果发现不适用于您的用例，则将其标记为无关紧要，或者使用严重性来确定首先要解决的问题的优先顺序。

调查结果可能具有以下状态：

- 打开 -需要注意。
- 已解决 -问题已修复。下一次评估将验证该修复程序。
- 无关紧要 — 被客户压制。在未来的评估中，这一发现一直被压制。

将发现标记为已解决 (CLI)

```
aws resiliencehubv2 update-failure-mode-finding \
  --service-arn "arn:aws:resiliencehub:..." \
  --finding-id "finding-123" \
  --status "RESOLVED"
```

将发现标记为无关紧要 (CLI)

```
aws resiliencehubv2 update-failure-mode-finding \
  --service-arn "arn:aws:resiliencehub:..." \
  --finding-id "finding-123" \
  --status "IRRELEVANT"
```

评估历史和趋势

下一代 Resilience Hub 可保留 2 年的评估历史记录，使您能够：

- 跟踪您的弹性姿势如何随着时间的推移而得到改善。
- 查看哪些调查结果已得到解决与保持开放状态。
- 确定评估中反复出现的问题。
- 生成显示改进趋势的合规性报告。

查看评估历史记录 (CLI)

```
aws resiliencehubv2 list-failure-mode-assessments \
  --service-arn "arn:aws:resiliencehub:..."
```

定价

每项服务包括每月 2 次故障模式评估，对于最多包含 150 个资源的服务，每项服务每月基本收费 15 美元。

对于超过 150 个资源的服务，所包含的 2 项评估均按超过 150 个资源门槛的每项资源收费 0.10 美元。除每月包含的2次评估外，其他评估将按相同的每项资源费率收费，每次评估至少收取50个资源。

服务规模	2 次评估的每月费用
100 个资源	15 美元（包括在内）
150 个资源	15 美元（包括在内）
200 个资源	15 美元 + (50 x 0.10 美元 x 2) = 25 美元
500 个资源	15 美元 + (350 x 0.10 美元 x 2) = 85 美元

弹性测试

在下一代 Resilience Hub 中， AWS 推荐了四种测试模板，这些模板旨在帮助您验证服务运行并在出现故障时按预期恢复。三项测试对应 AWS 故障隔离边界（可用区域和区域），并提供了一种一致的方法来测试您的服务对限于这些边界的故障的恢复能力。还有一项额外的测试可以帮助您验证您的服务在依赖项出现故障时可以恢复。每个测试都建立在 AWS Fault Injection Service (AWS FIS) 之上，它执行底层故障注入。下一代 Resilience Hub 将测试范围限定为服务中的资源，并根据您选择的成功标准评估结果，以确定通过或失败的结果。您在服务级别运行弹性测试。

主题

- 弹性测试的工作原理
- 配置测试
- 可用测试
- 测试运行和报告
- 用于弹性测试的 IAM 执行角色

弹性测试的工作原理

弹性测试使用三个核心概念：

- 测试模板 — 预先配置的推荐测试，用于定义要验证的弹性能力。测试模板指定要执行的操作，并声明其接受的参数。
- 测试 — 通过为服务配置推荐的测试模板（包括成功标准、停止条件和其他设置）来创建的测试。每项服务对每个模板都有一个测试。例如，为您的结账服务配置了“可用区：恢复测试”，RTO 为 30 分钟（恢复时间目标）。
- 测试运行 -单次执行测试。每个测试运行的范围均限定为服务中的当前资源，并生成通过或失败后果以及结果和报告。您可以多次运行同一个测试。例如，每月运行“可用区：恢复”测试，以测试 30 分钟 RTO 内的恢复情况。

当您运行弹性测试时，下一代 Resilience Hub 将执行以下操作：

1. 确定测试范围 -自动包括在您的服务中发现的适用于测试的所有资源。
2. 配置测试 -使用您提供的配置设置测试，包括成功警报、停止条件和日志目的地。
3. 注入故障 -运行 AWS FIS 实验，在指定的时间段内注入测试定义的故障。

4. 评估结果 -根据您的服务在测试期间是否满足成功标准来确定通过或失败的结果。您可以在控制台中查看测试结果，也可以通过编程方式查看测试结果。每次运行都会生成测试报告。

弹性测试根据 AWS FIS 行动分钟定价收费。有关详细信息，请参阅 AWS Fault Injection Service 定价。

配置测试

当您使用模板创建测试时，需要配置以下设置。设置已保存并重复使用以备将来运行时使用，您可以随时对其进行编辑。

测试持续时间

测试操作运行的时间长度。对于恢复测试（可用区域：恢复和 Multi-Region：恢复），默认时长为 RTO 加上 30 分钟，让您的服务有时间恢复并确认其持续性。对于持续测试，依赖关系验证的默认值为 30 分钟，隔离的默认值Multi-Region为 3 小时。这些默认值适用于控制台；使用 API 时，您需要明确提供持续时间。

故障范围

定义错误注入的位置——可用区域或要损害的区域。每个测试都有自己的参数。有关更多信息，请参阅 可用测试。

测试动作

Read-only。由测试模板定义。显示故障操作及其目标资源类型。如果没有资源与操作的目标类型相匹配，则跳过该操作。

要封锁的依赖关系

测试期间要屏蔽的依赖关系。从已发现的依赖关系（如果启用依赖项发现）中进行选择，或按 DNS 域名手动输入依赖关系。某些测试为必填项，其他测试为可选。有关默认值和要求，请参阅可用测试。

测试警报

成功警报（必填）— 确定成功标准通过或失败的 CloudWatch 警报。至少需要选择一个选项。如果选择多项，则必须全部通过才能通过测试。选择衡量服务整体运行状况的警报。

测试如何通过：

- 可用区：恢复 — 所有成功警报都必须恢复到您的 Multi-AZ RTO 内的0K状态，并保持该状态直到测试操作结束。

- Multi-Region: recov ery — 所有成功警报都必须恢复到您的 Multi-Region RTO 内的0K状态，并保持该状态直到测试操作结束。
- 依赖关系验证 — 所有成功警报都保持0K状态，直到测试操作结束。
- Multi-Region: 隔离 — 所有成功警报保持0K状态，直到测试操作结束。

其他警报（可选）-仅用于可观察性。显示在结果和报告中，但不影响及格或不及格结果。

区域切换计划（Multi-Region仅限恢复，可选）

附加 AWS 应用程序恢复控制器 (ARC) 区域切换计划可让下一代 Resilience Hub 将故障转移时间表纳入您的测试结果和报告。可选；如果您使用手动故障转移或自定义自动化，请留空。

其他设置（可选）

停止条件

CloudWatch 警报器会在突破阈值时自动停止测试。使用停止条件作为护栏，在测试期间保护您的工作负载。例如，针对关键业务指标（例如延迟或错误率）创建 CloudWatch 警报，该警报将在超过不可接受的阈值时停止测试。停止条件警报必须位于运行测试的账户和故障注入的区域中。有关更多信息，请参阅的停止条件 AWS FIS。

Reports

在您的服务上配置报告目的地（Amazon S3 存储桶）后，每次测试运行后都会自动生成报告。报告包括测试配置、警报状态、时间表以及通过或失败的结果。当您使用下一代的 Resilience Hub 弹性测试时，将免费提供测试报告。要配置报告目的地，请参阅服务的报告设置。

日志

向 Amazon S3 和/或两者发送详细的测试 CloudWatch 日志。日志捕获带有时间戳的事件，包括操作开始和结束、目标解析和错误。使用日志来调试失败的测试或了解故障注入的顺序。日志记录需要对您的测试执行角色拥有额外的权限。有关更多信息，请参阅的实验日志 AWS FIS。

测试权限

需要 IAM 执行角色。权限因测试类型、错误操作和所选选项而异。对于多账户测试，请在每个账户中使用同名角色。有关更多信息，请参阅 用于弹性测试的 IAM 执行角色。

可用测试

下一代 Resilience Hub 提供以下预配置的测试模板：

- 可用区：恢复 -验证您的服务是否可以检测到可用区损坏并从中恢复。

- 依赖关系验证 — 验证您的服务在区域内的依赖关系受损时如何响应。
- Multi-Region: 隔离 — 当无法连接到另一个区域时，验证您的服务是否可以独立于某个区域运行。
- Multi-Region: 恢复 — 验证当某个区域受损时，您的服务能否在恢复目标范围内从另一个区域恢复和服务客户。

每个测试模板都声明其接受的参数，包括每个参数是否为必填参数以及任何默认值。

列出测试模板 (CLI)

```
aws resiliencehubv2 list-test-templates --region region
```

查看测试模板 (CLI)

`get-test-template`用于查看测试模板的完整定义。 响应包括以下内容：

- 操作 -测试执行的操作，每个操作都针对特定的资源类型。
- 参数 -您在根据模板创建测试时提供的输入。

每项操作都包括以下内容：

- ActionID — 操作的唯一标识符。
- 描述 — 对操作功能的描述。
- ResourceType — 操作目标资源的类型。

每个参数声明以下内容：

- 名称 — 您在创建测试时提供的参数名称。
- 描述 — 对参数控制内容的描述。
- 类型 -值类型：`STRING`、`STRING_LIST`或`INTEGER`。
- 必填 —是否必须为参数提供值。
- 默认值 -不提供值时使用的值。适用于可选参数。
- 最大值 -您可以为参数提供的最大值数。

```
aws resiliencehubv2 get-test-template \
```

```
  --test-template-arn "arn:aws:resiliencehub:region:aws:test-template/aws-az-
recovery:rtaz001" \
  --region region
```

创建测试时，使用--parameters选项为这些参数提供值。有关创建测试的示例，请参阅下一代弹性中心入门。

主题

- 可用区：恢复
- 依赖关系验证
- Multi-Region: 隔离
- Multi-Region: 恢复

可用区：恢复

可用区：恢复测试会在单个可用区中注入电源中断的症状，从而影响该可用区内的计算、网络、存储和数据库资源。它可以帮助您验证您的服务是否检测到受损可用区，继续在运行正常的可用区中运行，并在定义的 RTO 内恢复到正常状态。此外，此测试可以帮助您显示您可能不知道的单可用区依赖关系。

是什么让这个测试与众不同

- 以您选择的单个可用区为目标，重点关注区域内弹性。
- 这是一项恢复测试——您的服务必须在 RTO 内恢复。

如何通过这个测试

- 这是一项恢复测试。RTO 倒计时从测试操作开始时开始。如果所有成功警报都恢复到您的 RTO 内的OK状态并保持该状态直到测试操作结束，则测试通过。

需要考虑的事情

- 选择衡量区域服务运行状况（例如，区域错误率、延迟）的成功警报——避免按可用区发出警报，因为受损的可用区预计会出现不健康状况。
- 对于流量可以转移到健康可用区的多可用区架构来说最有意义。也可以针对单可用区服务运行。
- 如果您在资源上启用了 AWS 应用程序恢复控制器 (ARC) 区域自动移动，则测试会自动切换。如果未配置自动移动，则会跳过该操作。

关键测试参数

- 可用区 -选择要削弱的可用区。选择您的服务已部署资源的可用区。
- 持续时间 -测试操作运行的时间长度。之后还需要几分钟才能在测试结束之前收集最终结果。默认为服务策略中的 RTO 加上首次创建测试时的 30 分钟。将其设置为比 RTO 更长的时间，以验证恢复是否持续。

操作

此测试运行以下 AWS FIS 操作来损害您选择的可用区。如果您的服务没有与操作目标类型相匹配的资源，则会跳过该操作。有关每个操作的详细信息，请参阅AWS FIS 操作参考。

处理建议	说明
aws:ec2:stop-instances	在一段时间内停止受损可用区中的实例。
aws:ec2:api-insufficient-instance-capacity-error	阻止在受损可用区启动新实例。
aws:ec2:asg-insufficient-instance-capacity-error	防止 Auto Scaling 在 AZ 中配置容量。
aws:network:disrupt-connectivity	阻止进入和离开子网的流量，并封锁对 Amazon S3 Express One Zone 目录存储桶（如果有）的访问。
aws:rds:failover-db-cluster	如果写入器位于受损可用区，则对群集进行故障切换。
aws:elasticache:replicationgroup-interrupt-az-power	在此期间终止受损可用区中的缓存节点，无需更换。
aws:arc:start-zonal-autoshift	将流量转移到健康的可用区。

要查看此测试的参数及其默认值，请使用get-test-template。

依赖关系验证

依赖关系验证测试会阻止该区域内的依赖关系，以查看您的服务在不可用时的行为。它可以帮助你验证在软依赖关系受损时你的服务是否保持健康，而你可能不知道的表面依赖关系很难。您还可以包括已知的硬依赖关系，以了解其影响。

是什么让这个测试与众不同

- 重点关注区域内依赖关系故障。
- 您可以选择将哪些依赖项作为目标。
- 如果您在下一代 Resilience Hub 中启用了依赖关系发现，则可以从已发现的依赖项中进行选择。否则，您可以手动输入 DNS 终端节点。

如何通过这个测试

- 这是一次持续的考验。如果所有成功警报都保持0K状态直到测试操作结束，则测试通过。使用它来验证软依赖关系是真正的软依赖关系——如果你的警报被破坏，这种依赖关系实际上可能很难。

需要考虑的事情

- 从单个软依赖关系开始，然后逐步建立一个软依赖关系，然后再屏蔽多个软依赖关系。
- 如果您包含硬依赖关系，则预计警报会被破坏，测试失败——硬依赖关系在被封锁时会产生重大影响。这对于确认依赖关系确实很困难很有用。
- 选择衡量整体服务运行状况的成功警报，而不是依赖项本身的运行状况。
- 确保在测试期间积极使用您的依赖关系（流量流向它们），这可以验证区块是否有效。考虑添加跟踪依赖关系使用情况（例如，请求数或连接错误）的警报或指标，以验证在测试期间是否使用了依赖关系。
- 依赖关系必须是可解析的 DNS 终端节点，如果 DNS 无法解析，操作将失败。
- 屏蔽触发运行状况检查失败的依赖关系可能会导致计算（例如 Amazon ECS 任务）被替换。丢包操作不会重新应用于替换任务，可能会报告为失败。

关键测试参数

- 持续时间 -测试操作运行的时间长度。之后还需要几分钟才能在测试结束之前收集最终结果。首次创建测试时的默认值为 30 分钟。

- 要屏蔽的依赖关系 -默认情况下，预先选择已发现的具有最大查询量的软依赖关系。如果没有将任何依赖关系归类为软依赖关系，则不选择任何依赖关系。您可以进行调整以定位单个依赖项或特定群组，也可以按 DNS 域名手动添加依赖关系。此处添加的其他依赖项仅用于此测试，不会保存到服务的依赖项发现中。这些默认值适用于控制台；使用 API 时，您可以明确提供依赖关系。

操作

此测试运行以下 AWS FIS 操作以减少流向您选择的依赖项的流量。操作会给亚马逊 EC2 实例、亚马逊 ECS 任务（亚马逊 EC2 和 Fargate）和亚马逊 EKS 容器（亚马逊 EC2）注入 100% 的数据包丢失。如果您的服务没有与操作目标类型相匹配的资源，则会跳过该操作。

> **Note**
>
> 用于阻止依赖关系的操作需要额外的设置：安装在亚马逊 EC2 实例上的 SSM 代理、亚马逊 ECS 任务定义中的 SSM 代理容器或亚马逊 EKS 容器的 Kubernetes 服务账户。

处理建议	说明
`aws:ssm:send-command`	将流量从 Amazon EC2 实例转移到所选依赖项。
`aws:ecs:task-network-packet-loss`	将流量从 Amazon ECS 任务转移到选定的依赖关系。
`aws:eks:pod-network-packet-loss`	将流量从亚马逊 EKS Pod 转移到选定的依赖项。

要查看此测试的参数及其默认值，请使用`get-test-template`。

Multi-Region: 隔离

Multi-Region: 隔离测试会阻止两个区域之间的连接，包括网络流量、跨区域数据复制和选定的依赖关系。它可以帮助您在无法访问其他区域的资源时验证您的服务是否独立运行，并显示可能影响可用性的跨区域依赖关系。

是什么让这个测试与众不同

- 重点是区域隔离（跨区域连接中断），而不是恢复到另一个区域。

- 阻止网络流量，暂停跨区域复制（Amazon S3、DynamoDB、MemoryDB），并可选择阻止两个区域之间的依赖关系。
- 验证该区域是否可以自行运行。

如何通过这个测试

- 这是一次持续的考验。如果所有成功警报都保持0K状态直到测试操作结束，则测试通过。

需要考虑的事情

- 选择衡量隔离区域运行状况的成功警报——验证该区域是否继续独立提供流量。
- 此测试适用于 active/active 和 active/passive 架构。
- 一个关键用例：验证您的恢复区域可以独立运行。例如，如果您的主服务器是us-east-1，次要是us-west-2，则使用它来验证与之隔离时是否独立us-west-2运行us-east-1。
- 该测试也是一个很好的前提条件 Multi-Region：恢复 ——在测试完全故障转移之前验证独立性。该测试可以帮助发现至关重要的跨区域依赖关系。
- 确保在测试期间积极使用您的依赖关系（流量流向它们），这可以验证区块是否有效。考虑添加跟踪依赖关系使用情况（例如，请求数或连接错误）的警报或指标，以验证在测试期间是否使用了依赖关系。
- 依赖关系必须是可解析的 DNS 端点。
- 屏蔽触发运行状况检查失败的依赖关系可能会导致计算（例如 Amazon ECS 任务）被替换。丢包操作不会重新应用于替换任务，可能会报告为失败。

关键测试参数

- 隔离区域 -您正在测试的独立运行区域。
- 目标区域 -被封锁的区域（与该区域的连接中断）。
- 持续时间 -测试操作运行的时间长度。之后还需要几分钟才能在测试结束之前收集最终结果。首次创建测试时的默认值为 3 小时。
- 要封锁的依赖关系（可选）-如果启用依赖项发现，则列表会显示从隔离区域到目标区域的依赖关系。您可以从该列表中选择，也可以按 DNS 域名手动添加。默认情况下不选择任何依赖关系。无论如何，此测试中的其他操作（网络连接、复制暂停）都会运行。此处添加的其他依赖项仅用于此测试，不会保存到服务的依赖项发现中。这些默认值适用于控制台；使用 API 时，您可以明确提供依赖关系。

操作

此测试运行以下 AWS FIS 操作以减少流向您选择的依赖项的流量。操作会给亚马逊 EC2 实例、亚马逊 ECS 任务（亚马逊 EC2 和 Fargate）和亚马逊 EKS 容器（亚马逊 EC2）注入 100% 的数据包丢失。如果您的服务没有与操作目标类型相匹配的资源，则会跳过该操作。

> **Note**
>
> 用于阻止依赖关系的操作需要额外的设置：安装在亚马逊 EC2 实例上的 SSM 代理、亚马逊 ECS 任务定义中的 SSM 代理容器或亚马逊 EKS 容器的 Kubernetes 服务账户。

处理建议	说明
`aws:network:transit-gateway-disrupt-cross-region-connectivity`	阻止通过 Transit Gateway 对等连接到达目标区域的跨区域流量。
`aws:network:route-table-disrupt-cross-region-connectivity`	阻止从子网到目标区域的跨区域流量。
`aws:network:disrupt-vpc-endpoint`	阻止流向目标区域的跨区域 VPC 终端节点的流量。
`aws:s3:bucket-pause-replication`	暂停向目标区域的 Amazon S3 跨区域复制。
`aws:dynamodb:global-table-pause-replication`	暂停 DynamoDB 全局表复制。
`aws:memorydb:multi-region-cluster-pause-replication`	暂停 MemoryDB 多区域集群复制。
`aws:ssm:send-command`	将流量从 Amazon EC2 实例转移到所选依赖项。
`aws:ecs:task-network-packet-loss`	将流量从 Amazon ECS 任务转移到选定的依赖关系。

处理建议	说明
aws:eks:pod-network-packet-loss	将流量从亚马逊 EKS Pod 转移到选定的依赖项。

要查看此测试的参数及其默认值，请使用get-test-template。

Multi-Region: 恢复

Multi-Region: recovery 测试会将失败引入一个区域的依赖关系，以验证您的服务能否在恢复目标范围内从恢复区域恢复和为客户提供服务。此测试适用于 active/active 和 active/passive 架构。例如，您可以启动恢复程序并确认您的服务在恢复区域中定义的恢复时间目标 (RTO) 内恢复。

是什么让这个测试与众不同

- 根据您的恢复目标（而不仅仅是区域内弹性）来验证向另一个区域的恢复。
- 您可以选择在主要区域中削弱哪些依赖关系，这样您就可以练习检测和恢复。
- 该测试与 ARC 区域开关集成，因此您可以在测试报告中跟踪计划执行的详细信息。

如何通过这个测试

- 这是一项恢复测试。RTO 倒计时从测试操作开始时开始。如果所有成功警报都恢复到您的 Multi-Region RTO 内的0K状态并保持该状态直到测试操作结束，则测试通过。您的服务必须具有定义了 Multi-Region RTO 的弹性策略。

需要考虑的事情

- 在受损地区选择足够重要以触发恢复程序的依赖关系。选择硬依赖关系或 DNS 终端节点，这些依赖项如果被封锁，将对该地区造成重大损害。
- 该测试会在受损区域注入故障——您可以自己执行恢复操作（例如，触发 failover/ARC 区域切换计划）。该测试通过评估警报状态来观察您的恢复区域在 RTO 内是否处于正常状态。
- 在恢复区域选择成功警报来验证其服务流量，或者使用反映整体客户体验的 global/application级别警报。
- 考虑将持续时间设置为比 RTO 更长的时间，以验证恢复是否持续。

- 确保在测试期间积极使用您的依赖关系（流量流向它们），这可以验证区块是否有效。考虑添加跟踪依赖关系使用情况（例如，请求数或连接错误）的警报或指标，以验证在测试期间是否使用了依赖关系。
- 依赖关系必须是可解析的 DNS 端点。
- 屏蔽触发运行状况检查失败的依赖关系可能会导致计算（例如 Amazon ECS 任务）被替换。丢包操作不会重新应用于替换任务，可能会报告为失败。

关键测试参数

- 受损区域 -故障注入的区域。
- 恢复区域 -您期望服务恢复到的区域。
- 持续时间 -测试操作运行的时间长度。之后还需要几分钟才能在测试结束之前收集最终结果。默认为服务策略中的 Multi-Region RTO 加上首次创建测试时的 30 分钟。
- 要屏蔽的依赖关系 -选择如果被封锁，将严重损害您的服务并有助于验证向其他区域的故障转移的依赖关系。默认情况下，已发现的具有最大查询量的硬依赖项是预先选择的。如果没有将依赖关系归类为硬依赖关系，则不选择任何依赖关系。您可以通过 DNS 域名调整或手动添加依赖关系。此处添加的其他依赖项仅用于此测试，不会保存到服务的依赖项发现中。这些默认值适用于控制台；使用 API 时，您可以明确提供依赖关系。
- 区域切换计划（可选）— 附加 ARC 区域交换机计划可让下一代 Resilience Hub 在测试结果和报告中包括实际的故障转移时间表。如果您使用手动故障转移或自定义自动化，请将其留空。

操作

此测试运行以下 AWS FIS 操作以减少流向您选择的依赖项的流量。操作会给亚马逊 EC2 实例、亚马逊 ECS 任务（亚马逊 EC2 和 Fargate）和亚马逊 EKS 容器（亚马逊 EC2）注入 100% 的数据包丢失。如果您的服务没有与操作目标类型相匹配的资源，则会跳过该操作。

> **Note**
>
> 用于阻止依赖关系的操作需要额外的设置：安装在亚马逊 EC2 实例上的 SSM 代理、亚马逊 ECS 任务定义中的 SSM 代理容器或亚马逊 EKS 容器的 Kubernetes 服务账户。

处理建议	说明
aws:ssm:send-command	将流量从 Amazon EC2 实例转移到所选依赖项。
aws:ecs:task-network-packet-loss	将流量从 Amazon ECS 任务转移到选定的依赖关系。
aws:eks:pod-network-packet-loss	将流量从亚马逊 EKS Pod 转移到选定的依赖项。

要查看此测试的参数及其默认值，请使用get-test-template。

测试运行和报告

测试运行

每次开始测试时，都会创建一次测试运行。你可以在多个地方查看测试运行情况：

- 服务级别：导航到您的服务 → 测试选项卡 → 底部的测试运行。显示该服务的所有运行次数。
- 测试运行页面（左侧导航）：显示所有服务的测试运行情况。按服务、测试名称或状态筛选。
- 控制面板：测试结果图表显示整个组织的 pass/fail分布情况。

每次测试运行都包括测试状态、计时信息、成功警报结果、操作时间表以及在运行期间屏蔽的任何依赖关系或记录事件。您可以深入测试以查看完整的详细信息，包括 AWS FIS 实验 ID 和个人操作结果。

您可以多次运行同一个测试。例如，每月运行 “可用区：恢复测试”，以跟踪一段时间内的弹性改善。您还可以使用和 GetTestRun API 操作以编程方式列出测试运行ListTestRuns并检索测试运行的详细信息。请参阅 API 参考。

测试报告

如果您的服务上配置了报告目的地（Amazon S3 存储桶），则每次测试运行完成后，会自动生成测试报告。如果未配置目标，则不会生成任何报告。

报告记录了测试配置、成功标准结果、服务响应情况的可视时间表以及总体 pass/fail 结果。

在哪里可以找到报告：

- 报告页面（左侧导航）：显示所有服务的报告（评估和测试）。
- 测试运行详情：直接从测试运行详情页面下载。

使用下一代 Resilience Hub 弹性测试时，免费包含测试报告。

您还可以使用和 `ListTestRunSources` API 操作以编程方式检索测试运行结果`GetTestRun`和报告元数据。请参阅 API 参考。

用于弹性测试的 IAM 执行角色

要运行弹性测试，您需要提供一个 IAM 执行角色，该 AWS Fault Injection Service 角色假定会向您的资源注入故障。AWS FIS你在测试中设置了这个角色，Resilience Hub 会在你开始测试时使用它。

当您在控制台中创建测试时，Resilience Hub 可以为您创建此角色。在您自己创建或自定义角色时使用本主题中的策略，例如使用 AWS CLI。

角色所需的权限取决于测试模板，因为每个模板运行一组不同的 AWS FIS 操作。本主题为四个测试模板提供了权限策略。有关模板的更多信息，请参阅可用测试。

Resilience Hub 支持两种账户模式：

- Single-account— 测试以运行实验的同一账户中的资源为目标。您创建一个执行角色。
- Multi-account— 测试的目标是其他账户中的资源。您在运行实验的账户中创建一个协调员角色，并在包含目标资源的每个账户中创建一个目标角色。

亚马逊建议您遵守授予最低权限的标准安全实践。以下策略将每种权限的范围限定为操作所针对的资源类型。弹性测试无法将权限范围限定为单个资源 ID，因为下一代 Resilience Hub 会在运行时解析目标资源。

主题

- Single-account 执行角色
- Multi-account 执行角色

Single-account 执行角色

对于单账户测试，请使用允许 AWS FIS 代入的信任策略和您使用的测试模板的权限策略创建一个执行角色。

信任策略

执行角色必须信任该 AWS FIS 服务。每个测试模板的信任策略都相同。aws:SourceAccount和aws:SourceArn条件可以防止出现混乱的副手问题，因此只有你的账户拥有的实验才能扮演这个角色。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "FISTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "fis.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:fis:*:account-id:experiment/*"
        }
      }
    }
  ]
}
```

权限策略

附上您的测试使用的测试模板的权限政策。

主题

- 可用区：恢复
- 依赖关系验证
- Multi-Region: 隔离
- Multi-Region: 恢复
- 创建角色并将其附加到您的测试中

可用区：恢复

可用区：恢复模板针对以下服务运行 AWS FIS 操作：亚马逊 EC2、亚马逊 EC2 Auto Scaling、亚马逊 ElastiCache、亚马逊 RDS、网络 ACL 和 AWS 应用程序恢复控制器区域转移。将以下权限策略附加到执行角色。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "EC2StopAndStartInstances",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "arn:aws:ec2:*:account-id:instance/*"
    },
    {
      "Sid": "EC2DescribeInstances",
      "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
    },
    {
      "Sid": "EC2EncryptedVolumesKmsGrant",
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:*:account-id:key/*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": ["Decrypt", "CreateGrant"]
        },
        "Null": {
          "kms:GrantOperations": "false"
        },
```

```
        "StringEquals": {
          "kms:GrantConstraintType": "EncryptionContextSubset"
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": "aws:ebs:id"
        }
      }
    },
    {
      "Sid": "EC2InjectApiError",
      "Effect": "Allow",
      "Action": "ec2:InjectApiError",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "ec2:FisActionId": [
            "aws:ec2:api-insufficient-instance-capacity-error",
            "aws:ec2:asg-insufficient-instance-capacity-error"
          ]
        }
      }
    },
    {
      "Sid": "AutoScalingDescribe",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ElastiCacheInterruptAzPower",
      "Effect": "Allow",
      "Action": [
        "elasticache:InterruptClusterAzPower",
        "elasticache:DescribeReplicationGroups"
      ],
      "Resource": "arn:aws:elasticache:*:account-id:replicationgroup:*"
    },
    {
      "Sid": "EBSPauseVolumeIO",
      "Effect": "Allow",
      "Action": "ec2:PauseVolumeIO",
```

```
      "Resource": "arn:aws:ec2:*:account-id:volume/*"
    },
    {
      "Sid": "EBSDescribeVolumes",
      "Effect": "Allow",
      "Action": "ec2:DescribeVolumes",
      "Resource": "*"
    },
    {
      "Sid": "NetworkTagManagedNacl",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*:account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkCreateManagedNacl",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkAcl",
      "Resource": "arn:aws:ec2:*:account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkCreateNaclOnVpc",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkAcl",
      "Resource": "arn:aws:ec2:*:account-id:vpc/*"
    },
    {
      "Sid": "NetworkModifyManagedNacl",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
```

```
      "Resource": "arn:aws:ec2:*:account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkDescribe",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeManagedPrefixLists"
      ],
      "Resource": "*"
    },
    {
      "Sid": "NetworkReplaceNaclAssociation",
      "Effect": "Allow",
      "Action": "ec2:ReplaceNetworkAclAssociation",
      "Resource": [
        "arn:aws:ec2:*:account-id:subnet/*",
        "arn:aws:ec2:*:account-id:network-acl/*"
      ]
    },
    {
      "Sid": "NetworkPrefixListEntries",
      "Effect": "Allow",
      "Action": "ec2:GetManagedPrefixListEntries",
      "Resource": "arn:aws:ec2:*:account-id:prefix-list/*"
    },
    {
      "Sid": "RDSFailoverCluster",
      "Effect": "Allow",
      "Action": [
        "rds:FailoverDBCluster",
        "rds:DescribeDBClusters"
      ],
      "Resource": "arn:aws:rds:*:account-id:cluster:*"
    },
    {
      "Sid": "RDSDescribeForTargetResolution",
```

```
      "Effect": "Allow",
      "Action": "rds:DescribeDBInstances",
      "Resource": "arn:aws:rds:*:account-id:db:*"
    },
    {
      "Sid": "ARCZonalShiftManagedElb",
      "Effect": "Allow",
      "Action": [
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:UpdateZonalShift",
        "arc-zonal-shift:CancelZonalShift"
      ],
      "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*",
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/net/*"
      ]
    },
    {
      "Sid": "ARCZonalShiftManagedAsgEks",
      "Effect": "Allow",
      "Action": [
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:UpdateZonalShift",
        "arc-zonal-shift:CancelZonalShift"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "arc-zonal-shift:ResourceIdentifier": [
            "arn:aws:autoscaling:*:account-id:autoScalingGroup:*",
            "arn:aws:eks:*:account-id:cluster/*"
          ]
        }
      }
    },
    {
      "Sid": "ARCZonalShiftList",
      "Effect": "Allow",
      "Action": "arc-zonal-shift:ListManagedResources",
      "Resource": "*"
    },
    {
```

```
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

依赖关系验证

依赖关系验证模板运行的 AWS FIS 操作可阻止来自亚马逊 EC2、亚马逊 ECS 和亚马逊 EKS 工作负载的区域内依赖流量。将以下权限策略附加到执行角色。

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

```
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:account-id:instance/*",
        "arn:aws:ssm:*:account-id:managed-instance/*",
        "arn:aws:ecs:*:account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Ec2DescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:account-id:task/*/*",
```

```
        "arn:aws:ecs:*:account-id:container-instance/*/*",
        "arn:aws:ecs:*:account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:account-id:cluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

Multi-Region: 隔离

Multi-Region: 隔离模板运行的 AWS FIS 操作会中断跨区域连接（路由表、传输网关和 VPC 终端节点），并暂停亚马逊 S3、亚马逊 DynamoDB 和 Amazon MemoryDB 的跨区域复制。将以下权限策略附加到执行角色。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "RouteTableDisruptCrossRegion",
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:CreateRoute"
      ],
      "Resource": [
        "arn:aws:ec2:*:account-id:route-table/*",
        "arn:aws:ec2:*:account-id:subnet/*"
      ]
    },
    {
      "Sid": "RouteTableManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateRouteTable",
      "Resource": "arn:aws:ec2:*:account-id:route-table/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "RouteTableManagedCreateOnVpc",
      "Effect": "Allow",
      "Action": "ec2:CreateRouteTable",
      "Resource": "arn:aws:ec2:*:account-id:vpc/*"
    },
    {
      "Sid": "RouteTableManagedDelete",
```

```
      "Effect": "Allow",
      "Action": "ec2:DeleteRouteTable",
      "Resource": [
        "arn:aws:ec2:*:account-id:route-table/*",
        "arn:aws:ec2:*:account-id:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "PrefixListManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateManagedPrefixList",
      "Resource": "arn:aws:ec2:*:account-id:prefix-list/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "PrefixListManagedModifyDelete",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteManagedPrefixList",
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource": "arn:aws:ec2:*:account-id:prefix-list/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaceManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": "arn:aws:ec2:*:account-id:network-interface/*",
      "Condition": {
        "StringEquals": {
```

```
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaceManagedCreateOnSubnetAndSg",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": [
        "arn:aws:ec2:*:account-id:subnet/*",
        "arn:aws:ec2:*:account-id:security-group/*"
      ]
    },
    {
      "Sid": "NetworkInterfaceManagedDelete",
      "Effect": "Allow",
      "Action": "ec2:DeleteNetworkInterface",
      "Resource": "arn:aws:ec2:*:account-id:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "FISCreateTags",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": [
        "arn:aws:ec2:*:account-id:route-table/*",
        "arn:aws:ec2:*:account-id:prefix-list/*",
        "arn:aws:ec2:*:account-id:network-interface/*",
        "arn:aws:ec2:*:account-id:security-group/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "Ec2NetworkDescribeAndRead",
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "TgwDisruptCrossRegion",
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable"
      ],
      "Resource": [
        "arn:aws:ec2:*:account-id:transit-gateway-route-table/*",
        "arn:aws:ec2:*:account-id:transit-gateway-attachment/*"
      ]
    },
    {
      "Sid": "VpcEndpointDisrupt",
      "Effect": "Allow",
      "Action": "ec2:ModifyVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:*:account-id:vpc-endpoint/*",
        "arn:aws:ec2:*:account-id:security-group/*"
      ]
    },
    {
      "Sid": "VpcEndpointSecurityGroupManaged",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress"
```

```
      ],
      "Resource": [
        "arn:aws:ec2:*:account-id:security-group/*",
        "arn:aws:ec2:*:account-id:vpc/*"
      ]
    },
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:account-id:instance/*",
        "arn:aws:ssm:*:account-id:managed-instance/*",
        "arn:aws:ecs:*:account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:account-id:task/*/*",
```

```
        "arn:aws:ecs:*:account-id:container-instance/*/*",
        "arn:aws:ecs:*:account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:account-id:cluster/*"
    },
    {
      "Sid": "DynamoDbGlobalTablePauseReplication",
      "Effect": "Allow",
      "Action": [
        "dynamodb:PutResourcePolicy",
        "dynamodb:GetResourcePolicy",
        "dynamodb:DeleteResourcePolicy",
        "dynamodb:DescribeTable",
        "dynamodb:InjectError"
      ],
      "Resource": "arn:aws:dynamodb:*:account-id:table/*"
    },
    {
      "Sid": "S3PauseReplicationConfiguration",
      "Effect": "Allow",
      "Action": [
        "s3:PutReplicationConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "BoolIfExists": {
          "s3:IsReplicationPauseRequest": "true"
        },
        "StringEquals": {
          "aws:ResourceAccount": "account-id"
        }
      }
    },
    {
      "Sid": "S3PauseReplication",
      "Effect": "Allow",
      "Action": "s3:PauseReplication",
      "Resource": "arn:aws:s3:::*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "account-id"
        }
      }
    },
    {
      "Sid": "S3ListAllBuckets",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "account-id"
        }
      }
    },
    {
      "Sid": "MemoryDbMultiRegionPauseReplication",
      "Effect": "Allow",
      "Action": [
        "memorydb:PauseMultiRegionClusterReplication",
        "memorydb:DescribeMultiRegionClusters"
      ],
      "Resource": "arn:aws:memorydb::account-id:multiregioncluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

Multi-Region: 恢复

Multi-Region: recov ery 模板运行在受损区域中阻止依赖流量的 AWS FIS 操作，以进行跨区域故障转移。将以下权限策略附加到执行角色。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:account-id:instance/*",
        "arn:aws:ssm:*:account-id:managed-instance/*",
        "arn:aws:ecs:*:account-id:task/*/*"
      ]
    },
    {
```

```
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Ec2DescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:account-id:task/*/*",
        "arn:aws:ecs:*:account-id:container-instance/*/*",
        "arn:aws:ecs:*:account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:account-id:cluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
```

```
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

创建角色并将其附加到您的测试中

将信任策略另存为`trust-policy.json`，将权限策略另存为`permissions-policy.json`，然后使用 AWS CLI 创建角色。

```
aws iam create-role \
  --role-name my-resilience-testing-role \
  --assume-role-policy-document file://trust-policy.json

aws iam put-role-policy \
  --role-name my-resilience-testing-role \
  --policy-name resilience-testing \
  --policy-document file://permissions-policy.json
```

在测试中设置角色，以便 Resilience Hub 将其用于测试运行。

```
aws resiliencehubv2 update-test \
  --test-id test-id \
```

```
  --role-name my-resilience-testing-role
```

Multi-account 执行角色

对于多账户测试，AWS FIS 使用角色链。AWS FIS 在运行实验的账户中担任协调员角色。然后，协调员角色在包含目标资源的每个账户中担任目标角色。创建一次协调员角色，然后在每个目标账户中创建一个目标角色。

Orchestrator 账户角色

在运行实验的账户中创建协调员角色。它的信任政策 AWS FIS 允许假设，其混淆代理保护与单账户信任政策相同。

信任策略

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "FISTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "fis.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "orchestrator-account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:fis:*:orchestrator-account-id:experiment/*"
        }
      }
    },
    {
      "Sid": "SelfAssume",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::orchestrator-account-id:role/orchestrator-role-name"
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

权限策略

每个测试模板的 Orchestrator 权限策略都相同。它允许该角色代入目标账户角色、解析目标以及管理实验记录和生命周期。在语句中列出每个目标账户角色的 ARN。AssumeTargetAccountRole

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "AssumeTargetAccountRole",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::target-account-id:role/target-role-name"
      ]
    },
    {
      "Sid": "FISExperimentLogging",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FISExperimentLogGroupAccess",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "FISExperimentLifecycle",
      "Effect": "Allow",
      "Action": [
        "fis:GetExperiment",
        "fis:StopExperiment",
        "fis:ListExperimentResolvedTargets"
      ],
      "Resource": "arn:aws:fis:*:orchestrator-account-id:experiment/*"
    },
    {
      "Sid": "OrchestratorTagGetResources",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    },
    {
      "Sid": "OrchestratorDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeRouteTables",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVolumes",
        "rds:DescribeDBClusters",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeCacheClusters",
        "ecs:DescribeTasks",
        "ecs:ListTasks",
        "ecs:DescribeServices",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeClusters",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeTable",
```

```
        "dynamodb:ListGlobalTables",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "elasticloadbalancing:DescribeLoadBalancers",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:GetManagedResource",
        "iam:GetRole",
        "iam:ListRoles",
        "s3:GetBucketTagging",
        "s3:ListAllMyBuckets",
        "s3:GetReplicationConfiguration",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": "*"
    }
  ]
}
```

目标账户角色

在包含目标资源的每个账户中创建目标角色。它的信任政策允许协调者角色代替它。该`sts:ExternalId`条件将假设操作限制为由 Orchestrator 账户拥有的 AWS FIS 实验。`aws:PrincipalArn`这种条件将信任与协调员的角色联系在一起。

信任策略

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "OrchestratorRoleAssumeRole",
      "Effect": "Allow",
      "Principal": {
        "AWS": "orchestrator-account-id"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "sts:ExternalId": "arn:aws:fis:*:orchestrator-account-id:experiment/*"
        },
```

```
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::orchestrator-account-id:role/orchestrator-
role-name"
        }
      }
    }
  ]
}
```

权限策略

附上您的测试使用的测试模板的权限政策。这些策略授予目标资源的故障注入权限。实验日志记录和生命周期权限由协调员角色授予，而不是目标角色授予。

主题

- 可用区：恢复
- 依赖关系验证
- Multi-Region: 隔离
- Multi-Region: 恢复

可用区：恢复

将以下权限策略附加到可用区的目标角色：恢复模板。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "EC2StopAndStartInstances",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "arn:aws:ec2:*:target-account-id:instance/*"
    },
    {
      "Sid": "EC2DescribeInstances",
      "Effect": "Allow",
```

```
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
    },
    {
      "Sid": "EC2EncryptedVolumesKmsGrant",
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:*:target-account-id:key/*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": ["Decrypt", "CreateGrant"]
        },
        "StringEquals": {
          "kms:GrantConstraintType": "EncryptionContextSubset"
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": "aws:ebs:id"
        }
      }
    },
    {
      "Sid": "EC2InjectApiError",
      "Effect": "Allow",
      "Action": "ec2:InjectApiError",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "ec2:FisActionId": [
            "aws:ec2:api-insufficient-instance-capacity-error",
            "aws:ec2:asg-insufficient-instance-capacity-error"
          ]
        }
      }
    },
    {
      "Sid": "AutoScalingDescribe",
      "Effect": "Allow",
      "Action": [
```

```
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ElastiCacheInterruptAzPower",
      "Effect": "Allow",
      "Action": [
        "elasticache:InterruptClusterAzPower",
        "elasticache:DescribeReplicationGroups"
      ],
      "Resource": "arn:aws:elasticache:*:target-account-id:replicationgroup:*"
    },
    {
      "Sid": "EBSPauseVolumeIO",
      "Effect": "Allow",
      "Action": "ec2:PauseVolumeIO",
      "Resource": "arn:aws:ec2:*:target-account-id:volume/*"
    },
    {
      "Sid": "EBSDescribeVolumes",
      "Effect": "Allow",
      "Action": "ec2:DescribeVolumes",
      "Resource": "*"
    },
    {
      "Sid": "NetworkTagManagedNacl",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*:target-account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkCreateManagedNacl",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkAcl",
      "Resource": "arn:aws:ec2:*:target-account-id:network-acl/*",
      "Condition": {
```

```
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkCreateNaclOnVpc",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkAcl",
      "Resource": "arn:aws:ec2:*:target-account-id:vpc/*"
    },
    {
      "Sid": "NetworkModifyManagedNacl",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource": "arn:aws:ec2:*:target-account-id:network-acl/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkDescribe",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeManagedPrefixLists"
      ],
      "Resource": "*"
    },
    {
      "Sid": "NetworkReplaceNaclAssociation",
      "Effect": "Allow",
      "Action": "ec2:ReplaceNetworkAclAssociation",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:subnet/*",
        "arn:aws:ec2:*:target-account-id:network-acl/*"
      ]
```

```
    },
    {
      "Sid": "NetworkPrefixListEntries",
      "Effect": "Allow",
      "Action": "ec2:GetManagedPrefixListEntries",
      "Resource": "arn:aws:ec2:*:target-account-id:prefix-list/*"
    },
    {
      "Sid": "RDSFailoverCluster",
      "Effect": "Allow",
      "Action": [
        "rds:FailoverDBCluster",
        "rds:DescribeDBClusters"
      ],
      "Resource": "arn:aws:rds:*:target-account-id:cluster:*"
    },
    {
      "Sid": "RDSDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": "rds:DescribeDBInstances",
      "Resource": "arn:aws:rds:*:target-account-id:db:*"
    },
    {
      "Sid": "ARCZonalShiftManagedElb",
      "Effect": "Allow",
      "Action": [
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:UpdateZonalShift",
        "arc-zonal-shift:CancelZonalShift"
      ],
      "Resource": [
        "arn:aws:elasticloadbalancing:*:target-account-id:loadbalancer/app/*",
        "arn:aws:elasticloadbalancing:*:target-account-id:loadbalancer/net/*"
      ]
    },
    {
      "Sid": "ARCZonalShiftManagedAsgEks",
      "Effect": "Allow",
      "Action": [
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:UpdateZonalShift",
        "arc-zonal-shift:CancelZonalShift"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "arc-zonal-shift:ResourceIdentifier": [
            "arn:aws:autoscaling:*:target-account-id:autoScalingGroup:*",
            "arn:aws:eks:*:target-account-id:cluster/*"
          ]
        }
      }
    },
    {
      "Sid": "ARCZonalShiftList",
      "Effect": "Allow",
      "Action": "arc-zonal-shift:ListManagedResources",
      "Resource": "*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    }
  ]
}
```

依赖关系验证

将以下权限策略附加到依赖关系验证模板的目标角色。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
```

```
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:instance/*",
        "arn:aws:ssm:*:target-account-id:managed-instance/*",
        "arn:aws:ecs:*:target-account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Ec2DescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:target-account-id:task/*/*",
        "arn:aws:ecs:*:target-account-id:container-instance/*/*",
        "arn:aws:ecs:*:target-account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
```

```
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:target-account-id:cluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    }
  ]
}
```

Multi-Region: 隔离

将以下权限策略附加到Multi-Region:隔离模板的目标角色。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Sid": "RouteTableDisruptCrossRegion",
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:CreateRoute"
      ],
      "Resource": [
        "arn:aws:ec2:*:target-account-id:route-table/*",
        "arn:aws:ec2:*:target-account-id:subnet/*"
      ]
    },
    {
      "Sid": "RouteTableManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateRouteTable",
      "Resource": "arn:aws:ec2:*:target-account-id:route-table/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
```

```
        }
      }
    },
    {
      "Sid": "RouteTableManagedCreateOnVpc",
      "Effect": "Allow",
      "Action": "ec2:CreateRouteTable",
      "Resource": "arn:aws:ec2:*:target-account-id:vpc/*"
    },
    {
      "Sid": "RouteTableManagedDelete",
      "Effect": "Allow",
      "Action": "ec2:DeleteRouteTable",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:route-table/*",
        "arn:aws:ec2:*:target-account-id:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "PrefixListManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateManagedPrefixList",
      "Resource": "arn:aws:ec2:*:target-account-id:prefix-list/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "PrefixListManagedModifyDelete",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteManagedPrefixList",
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource": "arn:aws:ec2:*:target-account-id:prefix-list/*",
      "Condition": {
        "StringEquals": {
```

```
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaceManagedCreate",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": "arn:aws:ec2:*:target-account-id:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaceManagedCreateOnSubnetAndSg",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:subnet/*",
        "arn:aws:ec2:*:target-account-id:security-group/*"
      ]
    },
    {
      "Sid": "NetworkInterfaceManagedDelete",
      "Effect": "Allow",
      "Action": "ec2:DeleteNetworkInterface",
      "Resource": "arn:aws:ec2:*:target-account-id:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "FISCreateTags",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:route-table/*",
        "arn:aws:ec2:*:target-account-id:prefix-list/*",
        "arn:aws:ec2:*:target-account-id:network-interface/*",
        "arn:aws:ec2:*:target-account-id:security-group/*"
```

```
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/managedByFIS": "true"
        }
      }
    },
    {
      "Sid": "Ec2NetworkDescribeAndRead",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "TgwDisruptCrossRegion",
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable"
      ],
      "Resource": [
        "arn:aws:ec2:*:target-account-id:transit-gateway-route-table/*",
        "arn:aws:ec2:*:target-account-id:transit-gateway-attachment/*"
      ]
    },
    {
      "Sid": "VpcEndpointDisrupt",
      "Effect": "Allow",
      "Action": "ec2:ModifyVpcEndpoint",
      "Resource": [
```

```
        "arn:aws:ec2:*:target-account-id:vpc-endpoint/*",
        "arn:aws:ec2:*:target-account-id:security-group/*"
      ]
    },
    {
      "Sid": "VpcEndpointSecurityGroupManaged",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource": [
        "arn:aws:ec2:*:target-account-id:security-group/*",
        "arn:aws:ec2:*:target-account-id:vpc/*"
      ]
    },
    {
      "Sid": "SsmSendCommandOnDocuments",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:instance/*",
        "arn:aws:ssm:*:target-account-id:managed-instance/*",
        "arn:aws:ecs:*:target-account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
```

```
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
        "arn:aws:ecs:*:target-account-id:task/*/*",
        "arn:aws:ecs:*:target-account-id:container-instance/*/*",
        "arn:aws:ecs:*:target-account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:target-account-id:cluster/*"
    },
    {
      "Sid": "DynamoDbGlobalTablePauseReplication",
      "Effect": "Allow",
      "Action": [
        "dynamodb:PutResourcePolicy",
        "dynamodb:GetResourcePolicy",
        "dynamodb:DeleteResourcePolicy",
        "dynamodb:DescribeTable",
        "dynamodb:InjectError"
      ],
      "Resource": "arn:aws:dynamodb:*:target-account-id:table/*"
    },
    {
      "Sid": "S3PauseReplicationConfiguration",
      "Effect": "Allow",
      "Action": [
        "s3:PutReplicationConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "BoolIfExists": {
          "s3:IsReplicationPauseRequest": "true"
```

```
        }
      }
    },
    {
      "Sid": "S3PauseReplication",
      "Effect": "Allow",
      "Action": "s3:PauseReplication",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "S3ListAllBuckets",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Sid": "MemoryDbMultiRegionPauseReplication",
      "Effect": "Allow",
      "Action": [
        "memorydb:PauseMultiRegionClusterReplication",
        "memorydb:DescribeMultiRegionClusters"
      ],
      "Resource": "arn:aws:memorydb::target-account-id:multiregioncluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    }
  ]
}
```

Multi-Region: 恢复

将以下权限策略附加到Multi-Region:恢复模板的目标角色。

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

```
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-Sources",
        "arn:aws:ssm:*::document/AWSFIS-Run-Network-Packet-Loss-ECS"
      ]
    },
    {
      "Sid": "SsmSendCommandOnInstances",
      "Effect": "Allow",
      "Action": "ssm:SendCommand",
      "Resource": [
        "arn:aws:ec2:*:target-account-id:instance/*",
        "arn:aws:ssm:*:target-account-id:managed-instance/*",
        "arn:aws:ecs:*:target-account-id:task/*/*"
      ]
    },
    {
      "Sid": "SsmListAndCancelCommands",
      "Effect": "Allow",
      "Action": [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Ec2DescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EcsDescribeForTargetResolution",
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:ListTasks"
      ],
      "Resource": [
```

```
        "arn:aws:ecs:*:target-account-id:task/*/*",
        "arn:aws:ecs:*:target-account-id:container-instance/*/*",
        "arn:aws:ecs:*:target-account-id:cluster/*"
      ]
    },
    {
      "Sid": "EksDescribeCluster",
      "Effect": "Allow",
      "Action": "eks:DescribeCluster",
      "Resource": "arn:aws:eks:*:target-account-id:cluster/*"
    },
    {
      "Sid": "TargetResolutionByTags",
      "Effect": "Allow",
      "Action": "tag:GetResources",
      "Resource": "*"
    }
  ]
}
```

创建角色并将其附加到您的测试中

在协调员账户中，创建协调员角色。

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

aws iam put-role-policy \
  --role-name my-orchestrator-role \
  --policy-name resilience-testing-orchestrator \
  --policy-document file://orchestrator-permissions-policy.json
```

在每个目标账户中，使用测试模板的权限策略创建目标角色。

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

aws iam put-role-policy \
  --role-name my-target-role \
  --policy-name resilience-testing-target \
```

```
  --policy-document file://target-permissions-policy.json
```

将协调器角色设置为测试的执行角色。

```
aws resiliencehubv2 update-test \
  --test-id test-id \
  --role-name my-orchestrator-role
```

仪表板和报告

下一代 Resilience Hub 仪表板提供组织弹性状况的集中视图，使 SRE 能够监控合规性、跟踪趋势并生成所有服务的报告。

主题

- 中央 SRE 控制面板概述
- Service-level 观点
- 按政策、账户、地区和系统筛选
- 生成合规性和弹性态势报告

中央 SRE 控制面板概述

仪表板是您了解各项服务的弹性的起点。它提供了以下功能：

- 弹性态势摘要 — 所有服务的总体合规状态
- 评估活动 — 最近和即将进行的评估
- 调查结果概述 — 按严重程度打开故障模式调查结果
- 依赖关系 -新发现或未分类的依赖关系
- 测试结果 — 所有服务的弹性测试 Pass/fail 状态

Service-level 观点

深入研究任何服务以查看有关其当前状态的详细信息。服务级别视图中提供了以下部分。

Section	它显示了什么
配置	输入来源、权限模型、关联系统和用户旅程
拓扑	资源和连接的可视化地图
故障模式	最新评估的故障模式调查结果，包括严重程度和状态
依赖项	已发现具有严重程度和允许状态的依赖关系
历史记录	评估历史和复原力分数趋势

按政策、账户、地区和系统筛选

您可以使用以下筛选器筛选仪表板视图。

筛选条件	说明
策略	仅显示使用特定弹性策略的服务
Account	专注于特定 AWS 账户中的服务
区域	筛选依据 AWS 区域
系统	显示特定系统中的服务
严重性	按严重性级别筛选故障模式调查结果
Compliance status	合规、不合规或未评估

对于 AWS 组织用户，可以使用以下其他过滤器：

- 组织单位 — 按 OU 筛选
- 会员账户 — 关注特定的成员账户

生成合规性和弹性态势报告

先决条件

在生成报告之前，您的服务必须具有：

- 一种报告输出配置，用于指定传送报告的 Amazon S3 存储桶。
- 一个调用者角色，信任下一代 Resilience Hub 服务，并有权写入已配置的 Amazon S3 存储桶。
- 至少完成了一项状态为的评估SUCCESS。

在创建或更新服务时，您可以配置报告输出：

```
aws resiliencehubv2 update-service \
  --service-arn "arn:aws:resiliencehub:us-east-1:123456789012:service/my-
service:abc123" \
  --report-configuration '{"reportOutputs": [{"s3": {"bucketPath": "my-report-bucket",
 "bucketOwner": "123456789012"}}]}'
```

调用者角色必须具有在目标存储桶s3:PutObject上授予的权限策略。以下示例显示了最低要求的策略。

```
{
  "Version": "2012-10-17"       ,
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-report-bucket/*"
    }
  ]
}
```

> **Note**
>
> 如果您的存储桶在中使用前缀bucketPath（例如，my-report-bucket/reports），请相应地设置资源范围（例如，arn:aws:s3:::my-report-bucket/reports/*）。

> **Note**
>
> 如果您的 Amazon S3 存储桶配置了 SSE-KMS 加密，则调用者角色还需要存储桶的 KMS 密钥kms:GenerateDataKey和kms:Encrypt权限。

生成故障模式评估报告

要在运行评估后生成报告，请执行以下操作：

1. 导航到您的服务。
2. 选择 “评估” 选项卡。
3. 选择生成报告。

试运行报告

如果配置了报告目标，则测试报告将在每次测试运行完成后自动生成。无需执行其他步骤。有关所含内容的详细信息，请参阅测试运行和报告。

查看报告

在左侧导航栏中，选择报告。报告页面显示您有权访问的所有生成的报告（失效模式评估和测试运行）。

AWS Organizations 集成

下一代 Resilience Hub 与 AWS Organizations 集成，可通过单个委派管理员 (DA) 账户实现组织范围的弹性管理。这样就无需登录个人账户来评估整个企业的弹性状况。无需登录个人账户，即可在整个组织范围内查看弹性态势和汇总仪表板。

指标	值
每个组织的账户数	50,000 +
跨组织的服务	10000
仪表板查询延迟	与组织规模无关
数据聚合延迟	少于 5 分钟

主题

- 下一代 Resilience Hub 中的多账户治理概述
- 设置组织集成

- Service-Linked 角色
- 跨账户应用弹性策略
- 查看组织范围的弹性状况
- 管理会员账号登录
- 委派管理员设置所需的 IAM 权限

下一代 Resilience Hub 中的多账户治理概述

下一代 Resilience Hub 可在整个 AWS 组织中实现集中式弹性治理。通过 Organizations 集成，您可以

- 通过单个仪表板查看所有账户的弹性状况。
- 创建和发布组织范围的弹性政策。
- 监控数百个账户和服务的合规性。
- 按账户 AWS 区域、组织单位 (OU) 和政策进行筛选。

以下核心概念适用于 Organizations 集成模型：

概念	说明
委派管理员	一个成员账户，用于管理整个组织的下一代 Resilience Hub
Org-level 政策	由 DA 创建的弹性政策，可在所有成员账户中查看和分配
Service-Linked 角色	在成员账户中自动创建，用于跨账户只读访问权限

在 AWS Organizations 中，授权的管理员

- 可以查看所有成员账户中的所有系统和服务。
- 通过将组织范围的弹性策略与共享系统上的用户旅程关联起来，创建和发布组织范围的弹性策略。
- 查看汇总的弹性态势仪表板。

Service-Linked 启用可信访问权限后，将在所有成员账户中自动创建角色 (SLR)，从而无需手动设置 IAM 即可为 DA 提供只读的跨账户可见性。

设置组织集成

要在 Organizations 中使用下一代 R AWS esilience Hub，您必须指定一个委托管理员帐户来管理组织范围内的策略和可见性。

先决条件

- AWS 必须将 Organizations 配置为启用所有功能。
- 您必须拥有管理账户的访问权限才能启用可信访问权限。
- 确定哪个成员账户将担任委托管理员。
- 管理账户必须创建 Service-Linked 角色 (SLR)，Organizations 集成才能正常运行。如果没有 SLR，则委托的管理员无法访问成员账户数据。

> **Important**
>
> 管理账户必须在设置过程中创建 Service-Linked 角色 (SLR)。如果没有 SLR，Organizations 集成就无法运行，并且在创建 SLR 之前，委托的管理员无法访问成员账户数据。

快速设置步骤

1. 在管理账户中，打开下一代弹性中心控制台，然后选择 AWS Organizations 设置。
2. 选中复选框以启用可信访问并创建 Service-Linked 角色 (SLR)。
3. 选择创建集成。
4. （可选）通过在同一页面上选择 “注册” 来注册委派管理员。
5. 从委托的管理员帐户中，在下一代 Resilition Hub 控制台中选择主区域。
6. 成员账户中的各个服务所有者为其服务创建自己的调用者角色。有关调用者角色设置的信息，请参阅。设置下一代弹性中心

安装完成后，下一代 Resilience Hub 将执行以下操作：

1. Service-Linked 角色是在所有成员账户中创建的。由于 API 限制，大型组织可能需要更多时间。
2. 下一代 Resilience Hub 获取了最初的组织结构。
3. DA 账户通过 SLR 获得跨账户可见性。

4. 组织结构同步开始（事件驱动加上 12 小时的协调工作）。

Service-Linked 角色

Service-Linked 角色 (AWSServiceRoleForResilienceHub) 是 IAM 角色，当您为管理账户启用可信访问权限时，会在每个成员账户resiliencehub.amazonaws.com中自动创建这些角色。这些角色为委派的管理员提供了对成员账户资源的只读跨账户可见性，无需手动配置 IAM。

SLR 是在新账户加入组织时自动创建的。

成员账户中的个人服务所有者仍会创建自己的调用者角色，用于对其服务进行评估。SLR 为 DA 提供跨账户可见性；它不会取代用于发现和评估的调用者角色。有关调用者角色设置的信息，请参阅。设置下一代弹性中心

跨账户应用弹性策略

管理账户或委托管理员可以通过将策略与系统关联，然后将成员账户中的服务与该系统关联来跨成员账户应用弹性策略。系统级策略适用于所有关联的服务。

1. 在管理账户或 DA 账户中创建弹性策略。
2. 创建系统并将策略与其关联。
3. 将成员账户中的服务关联到系统。

系统级策略适用于与该系统关联的所有服务，无论哪个成员账户拥有该服务。

查看组织范围的弹性状况

授权的管理员可以看到整个组织的聚合视图。组织仪表板显示：

- 所有账户的总体服务及其合规状态。
- 按组织内严重程度分列的调查结果摘要。
- 评估活动和趋势。
- 没有政策或近期评估的服务。

管理会员账号登录

会员账号入会通过 SLR 自动处理：

- 新账户 — 当一个新账户加入组织时，系统会在新账户中自动创建 SLR，该账户将显示在 DA 的组织视图中，DA 可以看到在新账户中创建的服务。
- 已删除的帐户-当帐户离开组织时，DA 将无法再看到该帐户的数据，并且已删除账户中的服务将继续独立运行。

委派管理员设置所需的 IAM 权限

Organizations 集成中的每个角色都需要以下 IAM 权限：

管理账户

管理账户需要以下权限：

- `organizations:EnableAWSServiceAccess`
- `organizations:RegisterDelegatedAdministrator`
- `iam:CreateServiceLinkedRole`（用于管理账户自己的单反相机）

委派管理员帐户

DA 账户使用标准的下一代 Resilience Hub API 权限。 Cross-account 访问由 SLR 处理 — 无需额外的 IAM 配置即可查看成员账户数据。

成员账号

成员账户中的服务所有者：

- 使用与单账户设置相同的流程创建自己的调用者角色。有关更多信息，请参阅 设置下一代弹性中心。
- 可以查看和应用 DA 发布的组织级别政策。
- SLR 会自动处理 DA 跨账户的可见性，无需在成员账户中进行额外的 IAM 更改。

下表汇总了 DA 能做什么和不能做什么：

处理建议	支持
查看成员账户服务、调查结果和依赖关系	是

处理建议	支持
创建引用成员服务的组织级系统	是
为组织级系统提供关联成员服务	是
创建组织级别的策略	是
删除成员账户服务	否
开始对会员服务进行评估	是
修改成员账户资源	否

不支持通过 DA 跨账户访问对成员资源进行破坏性操作。DA 管理组织级别的系统和政策，并查看成员数据。

迁移来源 AWS Resilience Hub

如果您是现有 AWS Resilience Hub (v1) 客户，本指南可帮助您了解下一代 Resilience Hub 的变化以及如何迁移应用程序。下表汇总了两个版本之间的主要变化。

区域图	AWS Resilience Hub v1	下一代弹性中心
原始核心	应用程序	系统 + 服务
评估引擎	基于静态规则的检查	GenAI-powered 失效模式分析
依赖关系可见性	无	依赖项发现
Multi-account	有限	全面 AWS 的组织集成
策略	每个应用程序只有一个 RTO/RPO 策略	模块化、可组合的策略（灾难恢复 + 可用性 + 数据恢复）
测试	AWS FIS 实验模板（手动设置）	推荐的弹性测试（预先配置、自动定向） pass/fail
API 版本	/v1	/v2

主题

- 下一代 Resilience Hub 有哪些变化
- 概念映射： AWS Resilience Hub v1 到下一代弹性中心
- Step-by-step 迁移指南
- 定价过渡
- 迁移期间的已知限制

下一代 Resilience Hub 有哪些变化

下一代 Resilience Hub 引入了新的应用程序建模层次结构、 GenAI-powered 评估和自动依赖项发现。本节总结了主要变化。

- 新的层次结构 — v1 的 “应用程序” 概念映射到 “服务” 作为主要评估单位。服务分组在系统内，用户旅程描述了通过这些服务的路径。
- GenAI-powered 失效模式评估 — 基于静态规则的检查被生成式 AI 分析所取代，该分析可根据您的架构特定的推理生成详细的故障模式结果。
- 依赖关系发现 — 下一代 Resilience Hub 会自动发现服务与外部资源之间的依赖关系，这是 v1 中不可用的功能。
- 模块化弹性策略 — 策略现在是可组合的。您可以将灾难恢复 (DR)、可用性 SLO 和数据恢复条件合并到一个策略中，而不是单 RTO/RPO 一对策略中。
- 全面 AWS 的组织集成 — 通过单个委托管理员账户进行 Organization-wide 管理取代了 v1 中有限的多账户支持。

概念映射： AWS Resilience Hub v1 到下一代弹性中心

下表将从 AWS Resilience Hub v1 的概念映射到下一代 Resilience Hub 中的等效概念。

AWS Resilience Hub v1 概念	下一代弹性中心概念	注意
应用程序	服务	您的 v1 “应用程序” 成为下一代 Resilience Hub “服务”，即评估的主要单位
弹性检查	失效模式评估结果	静态检查被带有推理的 GenAI-powered 调查结果所取代

AWS Resilience Hub v1 概念	下一代弹性中心概念	注意
应用程序评估	服务故障模式评估	同样的概念，现在处于服务级别，产出更丰富
评估政策 (RTO/RPO)	弹性政策（模块化）	策略现在是可组合的：灾难恢复 + 可用性 SLO + 数据恢复
应用程序（作为分组）	系统 + 用户旅程	应用程序的 “分组” 方面映射到系统和用户旅程
—（不可用）	依赖项发现	下一代 Resilience Hub 的新功能
—（不可用）	服务功能	服务中的技术工作流程；下一代 Resilience Hub 中的新功能

Step-by-step 迁移指南

按照以下步骤将现有的 AWS Resilience Hub v1 应用程序迁移到下一代 Resilience Hub。

确定要迁移的应用程序

使用 AWS Resilience Hub v1 API 查找要迁移的应用程序 ARN。

```
# List your v1 applications
aws resiliencehub list-apps
```

记下要迁移的应用程序的 ARN。在下一步骤中，您将使用此 ARN。

使用迁移 API

下一代 Resilience Hub 提供迁移 API，可为您处理过渡。`import-app`API 会自动创建服务——您无需先手动创建系统或服务。

```
# Import a v1 application to a next generation Resilience Hub service
aws resiliencehubv2 import-app \
  --v1-app-arn "arn:aws:resiliencehub:us-east-1:123456789012:app/my-app:..."

# Import a v1 policy to a next generation Resilience Hub policy
```

```
aws resiliencehubv2 import-policy \
  --v1-policy-arn "arn:aws:resiliencehub:us-east-1:123456789012:resiliency-policy/..."
```

迁移 API 执行以下操作：

- 从 v1 应用程序创建服务（在新系统或现有系统中）
- 保留您的输入源和资源配置
- 将您的 v1 策略转换为具有模块化条件的弹性策略
- 保留评估历史以保持连续性

进行首次故障模式评估

迁移后，运行故障模式评估以查看增强的输出。

```
aws resiliencehubv2 start-failure-mode-assessment \
  --service-arn "arn:aws:resiliencehub:..."
```

故障模式调查结果包括针对您的架构的详细推理、包含成本和复杂性指导的建议以及显示哪些需求存在风险的策略映射。

启用新功能

利用 v1 中不可用的功能。

1. 启用依赖关系发现 -发现服务与外部资源之间隐藏的依赖关系。
2. 设置组织 -在整个组织中启用多账户管理。
3. 添加性能条件 — 使用可用性 SLO 条件定义正常运行时间以外的 “可用” 含义。

定价过渡

下表显示了定价组件如何从 AWS Resilience Hub v1 映射到下一代 Resilience Hub。

组件	AWS Resilience Hub v1	下一代弹性中心
基本费用	$ 15/application /月	$ 15/service /月
包括评估	无限制	每月 2 个

组件	AWS Resilience Hub v1	下一代弹性中心
资源覆盖率	无	0 美元。10/resource 每次评估超过 150
依赖项发现	不可用	$ 10/service /月（可选）

15美元的入场价格得以保留。大多数客户（资源不超过 150 个的服务，每月评估 2 次或更少）支付的金额相同。

迁移期间的已知限制

在从 AWS Resilience Hub v1 向下一代 Resilience Hub 的迁移期间，以下限制适用。

限制	说明	解决办法
评估历史	v1 评估结果不会自动迁移到下一代 Resilience Hub 格式	在过渡期间，可通过 v1 API 访问 v1 结果
自定义弹性检查	v1 自定义检查未迁移	查看失效模式调查结果 — GenAI 评估通常涵盖相同的问题
AppRegistry 输入源	AppRegistry 下一代 Resilience Hub 不支持作为输入源	使用其他输入源，例如 CloudFormation 堆栈或资源标签

下一代弹性中心的安全性

的云安全 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组织的要求而构建的数据中心和网络架构。

安全是您 AWS 和您的共同责任。分担责任模型将其描述为云的安全性和云中的安全。

本主题介绍下一代 Resilenity Hub 的安全功能和最佳实践，包括 IAM 权限、数据加密、网络安全和审计日志。

主题

- IAM 角色和权限参考
- 数据加密

- VPC 端点
- CloudTrail 整合
- 合规性注意事项

IAM 角色和权限参考

IAM 在评估和弹性测试中的作用

要进行评估或弹性测试，下一代弹性中心需要能够担任 IAM 角色。评估需要只读权限才能发现和了解您的 AWS 资源配置。弹性测试还需要权限才能代表你启动和管理 AWS Fault Injection Service (AWS FIS) 实验。

您可以在 IAM 控制台中创建 AWS IAM 角色。选择自定义信任策略并使用如下信任策略：

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

要获得权限，请附加AWSResilienceHubV2AssessmentExecutionPolicy托管策略。该政策授予对用于弹性发现、评估和管理的 AWS 服务的只读访问权限。

> **Note**
>
> 它用下一AWSResilienceHubV2AssessmentExecutionPolicy代的 R AWSResilienceHubAsssessmentExecutionPolicy esilience Hub 取代了之前使用的版本。有关此策略中包含的权限的详细信息，请参阅AWSResilienceHubV2AssessmentExecutionPolicy。

如果您使用弹性测试，还要附上AWSResilienceHubResilienceTestingPolicy托管策略。该政策授予Resilience Hub代表您启动和管理实验所需的 AWS FIS 权限。

> **Note**
>
> 如果您的账户中没有该托管策略，请创建具有相同权限的内联策略。有关政策内容，请参阅AWSResilienceHubResilienceTestingPolicy。

IAM Service-Linked 角色

下一代 Resilience Hub 使用AWSResilienceHubServiceRolePolicy托管策略自动创建 Service-Linked 角色。

Terraform 状态文件访问权限

如果您将 Terraform 状态文件包含到下一代弹性中心服务中，请使用如下策略提供从亚马逊 S3 存储桶读取 Terraform 文件的权限：

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

IAM 在弹性测试中的执行角色

弹性测试在 IAM 角色下运行，该角色 AWS Fault Injection Service 假定会向您的资源注入故障。所需的权限取决于测试模板，单账户和多账户测试使用不同的角色结构。有关每项测试的信任和权限政策，请参阅用于弹性测试的 IAM 执行角色。

亚马逊 EKS 权限

如果您要将亚马逊 EKS 集群纳入您的下一代 Resilience Hub 服务，请遵循以下 3 步流程，提供下一代 Resilience Hub 权限，允许其使用 Kubernetes 基于角色的访问控制 (RBAC) 读取亚马逊 EKS 集群的配置数据。

第 1 步：将以下内容应用到您的 Amazon EKS 集群

这为下一代 Resilience Hub 提供了对所有命名空间所需的 Kubernetes 资源的只读访问权限：

```
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
    - services
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
```

```
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

第 2 步：将 IAM 角色映射到 Kubernetes 群组

将您创建的 IAM 角色映射到 `resilience-hub-eks-access-group` Kubernetes 群组。您可以使用亚马逊 EKS 访问条目（推荐）或 `aws-auth` ConfigMap.

选项 A：使用 EKS 访问条目（推荐）

EKS 访问条目是管理集群身份验证的首选方法。您的集群必须使用`API`或`API_AND_CONFIG_MAP`身份验证模式。

```
aws eks create-access-entry \
  --cluster-name cluster-name \
  --principal-arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole \
  --type STANDARD \
  --kubernetes-groups '["resilience-hub-eks-access-group"]'
```

选项 B：使用 aws-auth ConfigMap

如果您的集群使用`CONFIG_MAP`或`API_AND_CONFIG_MAP`身份验证模式，则可以改为编辑 aws-auth ConfigMap ：

使用 eksctl：

```
eksctl create iamidentitymapping \
  --cluster cluster-name \
  --region region \
  --arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole \
  --group resilience-hub-eks-access-group \
  --username AwsResilienceHubAssessmentEKSAccessRole
```

或者手动编辑 ConfigMap：

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

mapRoles在数据部分下方添加以下内容：

```
- groups:
    - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole
  username: AwsResilienceHubAssessmentEKSAccessRole
```

第 3 步：验证

确认 RBAC 资源存在且角色映射已到位：

```
kubectl get clusterrole resilience-hub-eks-access-cluster-role
kubectl describe clusterrolebinding resilience-hub-eks-access-cluster-role-binding
```

如果使用访问条目（选项 A）：

```
aws eks describe-access-entry \
  --cluster-name cluster-name \
  --principal-arn arn:aws:iam::ACCOUNT-ID:role/ResilienceHubRole
```

如果使用 aws-auth ConfigMap （选项 B）：

```
kubectl get configmap aws-auth -n kube-system -o yaml | grep -A 3 "ResilienceHubRole"
```

数据加密

下一代 Resilience Hub 对您的数据进行加密，以帮助保护其免受未经授权的访问。

静态加密

所有下一代 Resilience Hub 数据都经过静态加密。

数据存储	加密
DynamoDB 表	AWS-管理密钥（默认）或客户 AWS KMS 管理的密钥
S3 对象（拓扑、评估结果）	SSE-S3 （默认）或 SSE-KMS 使用客户管理的密钥

使用客户管理的密钥进行静态加密

下一代 Resilience Hub 默认提供加密，以保护敏感的静态客户数据 AWS 拥有的密钥。

- 默认情况下，下一代 Resilience Hub 使用这些密钥来自动加密敏感数据。您无法查看、管理 AWS 拥有的密钥、使用或审核其使用情况。不过，您不必采取任何措施或更改任何计划以保护对数据进行加密的密钥。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的 https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#aws-owned-cmk。

虽然您无法禁用此加密层或选择其他加密类型，但您可以通过在创建服务资源时指定客户托管密钥来添加第二层加密：

- 客户管理的密钥下一代 Resilience Hub 支持使用由您创建、拥有和管理的对称加密客户托管密钥。由于您可以完全控制这层加密，因此可以执行以下任务：
  - 制定和维护关键策略
  - 建立和维护 IAM 策略和授权
  - 启用和禁用密钥策略
  - 轮换加密材料
  - 添加 标签
  - 创建密钥别名
  - 安排密钥删除

  有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的客户托管密钥。

下表总结了下一代 Resilience Hub 如何加密敏感数据。

对下一代弹性中心中的数据类型进行加密

数据类型	AWS 自有密钥加密	客户托管密钥加密（可选）
`description` 服务、系统和弹性策略的描述。	已启用	已启用
`finding` 评估发现姓名、描述、推理和评论。	已启用	已启用
`recommendation` 与调查结果相关的建议描述和建议的更改。	已启用	已启用
`serviceFunction` 服务函数的名称和描述。	已启用	已启用
`assumption` 与服务函数相关的假设文本。	已启用	已启用
`userJourney` 用户旅程描述。	已启用	已启用
`event` 服务事件日志描述。	已启用	已启用
`assessmentData` 代理评估工作流程生成的中间数据，包括拓扑、资源配置和存储在 Amazon S3 中的工作数据。	已启用	已启用
资源标识符 资源名称、ARN、资源类型和区域。资源名称用于标识符和加密上下文，不得包含敏感数据。	已启用	不支持

> **Note**
>
> 下一代 Resilience Hub 可自动启用静态加密 AWS 拥有的密钥 ，不收取任何费用。但是，使用客户管理的密钥需要 AWS KMS 付费。有关定价的更多信息，请参阅 AWS Key Management Service 定价。

> **Important**
>
> 下一代弹性中心仅支持对称加密 KMS 密钥。您不能使用任何其他类型的 KMS 密钥来加密您的下一代 Resilience Hub 资源。有关确定 KMS 密钥是否为对称加密密钥的帮助，请参阅开发人员指南中的识别对称和非对称 KMS 密钥。AWS Key Management Service

下一代弹性中心如何使用补助金 AWS KMS

下一代 Resilience Hub 需要获得授权，才能在异步评估工作流程中使用您的客户托管密钥。

当您使用客户托管密钥创建服务时，下一代 Resilience Hub 会通过向发送CreateGrant请求来代表您创建授权 AWS KMS。该授权仅限于您的服务的加密上下文，并且仅允许以下操作：

- `Encrypt`— 加密敏感字段，例如评估工作流程中生成的调查结果、建议和假设。
- `Decrypt`— 在评估过程中解密先前加密的数据。
- `GenerateDataKey`— 生成数据密钥以加密存储在 Amazon S3 中的中间评估数据。

删除服务后，该授权即告失效。您也可以随时撤消对授予的访问权限，或者删除该服务对客户托管密钥的访问权限。如果这样做，下一代 Resilience Hub 将无法访问由客户托管密钥加密的任何数据，这会影响依赖该数据的 API 操作和评估工作流程。

对于同步 API 操作（例如创建或更新服务），下一代 Resilience Hub 无需授予即可直接使用调用者对 KMS 密钥的权限。

创建客户托管密钥

您可以使用 AWS 管理控制台 或 AWS KMS API 创建对称加密客户托管密钥。

创建对称加密客户托管密钥

请按照《AWS Key Management Service 开发人员指南》中创建对称加密 KMS 密钥的步骤操作。

为下一代弹性中心指定客户管理的密钥

您可以在创建服务、系统或弹性策略时指定客户托管密钥。当您提供 KMS 密钥 ID 时，下一代 Resilience Hub 会使用该密钥来加密与该资源关联的所有敏感数据。

您可以使用以下任意密钥标识符来指定密钥：

- 密钥 ID（例如，1234abcd-12ab-34cd-56ef-1234567890ab）
- 密钥 ARN（例如，）arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
- 别名（例如，alias/my-key）
- 别名 ARN（例如，）arn:aws:kms:us-west-2:111122223333:alias/my-key

要指定客户托管密钥，请在调用CreateServiceCreateSystem、或 CreatePolicy API 操作时使用kmsKeyId参数。

密钥策略

密钥策略控制对客户自主管理型密钥的访问。每个客户托管式密钥必须只有一个密钥策略，其中包含确定谁可以使用密钥以及如何使用密钥的声明。创建客户托管式密钥时，可以指定密钥策略。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的管理对客户托管密钥的访问。

以下密钥策略允许下一代 Resilience Hub 使用您的密钥。它使用加密上下文条件确保您的密钥只能用于您的特定资源，将每项权限的范围限定为下一代 Resilience Hub 所需的操作。用您的值替换*CUSTOMER-ACCOUNT-ID*CUSTOMER-ROLE、和*REGION*。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowResilienceHubDescribeKey",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": "kms:DescribeKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com"
                }
```

```
            }
        },
        {
            "Sid": "AllowResilienceHubEncryptDecryptForServices",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:resiliencehub:service-arn":
"arn:aws:resiliencehub:*:CUSTOMER-ACCOUNT-ID:service/*"
                }
            }
        },
        {
            "Sid": "AllowResilienceHubEncryptDecryptForSystems",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:resiliencehub:system-arn":
"arn:aws:resiliencehub:*:CUSTOMER-ACCOUNT-ID:system/*"
                }
```

```
            }
        },
        {
            "Sid": "AllowResilienceHubEncryptDecryptForPolicies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:resiliencehub:policy-arn":
"arn:aws:resiliencehub:*:CUSTOMER-ACCOUNT-ID:policy/*"
                }
            }
        },
        {
            "Sid": "AllowResilienceHubCreateGrantForAsyncWorkflows",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::CUSTOMER-ACCOUNT-ID:role/CUSTOMER-ROLE"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "resiliencehub.REGION.amazonaws.com",
                    "kms:GrantConstraintType": "EncryptionContextSubset"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:resiliencehub:service-arn":
"arn:aws:resiliencehub:*:CUSTOMER-ACCOUNT-ID:service/*"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Encrypt",
```

```
                    "Decrypt",
                    "GenerateDataKey"
                ]
            }
        }
    }
]
}
```

策略声明提供以下权限：

- AllowResilienceHubDescribeKey— 允许下一代 Resilience Hub 在服务创建期间指定密钥时验证您的密钥是否存在并且是对称加密密钥。
- AllowResilienceHubEncryptDecryptForServices— 允许下一代 Resilience Hub 在同步 API 调用期间加密和解密服务级别数据（发现、建议、假设、服务功能、事件和评估数据）。根据加密上下文限定您的服务资源。
- AllowResilienceHubEncryptDecryptForSystems— 允许下一代 Resilience Hub 在同步 API 调用期间加密和解密系统级数据（系统描述和用户旅程描述）。根据加密上下文限定您的系统资源。
- AllowResilienceHubEncryptDecryptForPolicies— 允许下一代弹性中心在同步 API 调用期间加密和解密策略级数据（弹性策略描述）。根据加密上下文限定您的策略资源。
- AllowResilienceHubCreateGrantForAsyncWorkflows— 允许下一代 Resilience Hub 为异步评估工作流程创建补助金。该授权仅限于所需的操作（加密、解密等 GenerateDataKey），并且必须包含绑定到您的服务 ARN 的加密上下文子集约束。

有关在策略中指定权限的更多信息，请参阅《AWS Key Management Service 开发人员指南》。

有关密钥访问故障排除的信更多息，请参阅《AWS Key Management Service 开发人员指南》。

下一代弹性中心加密上下文

加密上下文是一组可选的键值对，包含有关数据的其他上下文信息。

AWS KMS 使用加密上下文作为其他经过身份验证的数据来支持经过身份验证的加密。当您在加密数据的请求中包含加密上下文时，会将加密上下文 AWS KMS 绑定到加密数据。要解密数据，您必须在请求中包含相同的加密上下文。

下一代弹性中心加密上下文

下一代 Resilience Hub 根据资源类型使用以下加密上下文密钥：

加密上下文密钥

加密上下文密钥	Scope	用于
aws:resiliencehub:service-arn	服务	调查结果、建议、假设、服务功能、依赖关系、事件和评估数据
aws:resiliencehub:system-arn	系统	系统描述和用户旅程描述
aws:resiliencehub:policy-arn	Policy	弹性策略描述

服务级别操作的加密上下文示例：

```
"encryptionContext": {
    "aws:resiliencehub:service-arn": "arn:aws:resiliencehub:us-
west-2:111122223333:service/my-service:abc123"
}
```

使用加密上下文进行监控

当您使用对称加密客户托管密钥来加密数据时，您可以使用审计记录和日志中的加密上下文来识别客户托管密钥的使用情况。加密上下文显示在生成的日志中AWS CloudTrail。

使用加密上下文来控制访问权限

您可以使用密钥策略和 IAM 策略中的加密上下文conditions来控制对称加密客户托管密钥的访问权限。您也可以在授予中使用加密上下文约束。

下一代 Resilience Hub 在授权中使用加密上下文子集约束，以确保异步工作流程只能加密和解密属于为其创建的特定服务的数据。

监控下一代弹性中心的加密密钥

当您将客户托管密钥与下一代 Resilience Hub 资源一起使用时，您可以使用AWS CloudTrail来跟踪下一代 Resilience Hub 发送到的请求 AWS KMS。

CreateGrant

当您使用客户托管密钥创建服务时，下一代 Resilience Hub 会代表您发送CreateGrant请求，要求允许异步评估工作流程使用您的密钥。该授权特定于该服务，并受加密上下文的限制。下一代 Resilience Hub 用于RetireGrant在您删除服务时移除授权。

以下示例事件记录了 CreateGrant 操作：

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLE:session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/YourRole/session-name",
        "accountId": "111122223333",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/YourRole",
                "accountId": "111122223333",
                "userName": "YourRole"
            }
        },
        "invokedBy": "resiliencehub.amazonaws.com"
    },
    "eventTime": "2026-01-15T10:07:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "resiliencehub.amazonaws.com",
    "userAgent": "resiliencehub.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "resiliencehub.amazonaws.com",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "retiringPrincipal": "resiliencehub.amazonaws.com",
        "operations": [
            "Decrypt",
            "GenerateDataKey",
            "Encrypt"
        ],
        "constraints": {
```

```
            "encryptionContextSubset": {
                "aws:resiliencehub:service-arn": "arn:aws:resiliencehub:us-
west-2:111122223333:service/my-service:abc123"
            }
        }
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "56d4e434-abb6-4dd7-8558-ad38560d03b1",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

当下一代 Resilience Hub 使用您的客户托管密钥加密数据时，它会发送生成数据密钥的GenerateDataKey请求。这发生在同步 API 调用（例如创建带有描述的服务）和异步评估工作流程中。

以下示例事件记录了 GenerateDataKey 操作：

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "resiliencehub.amazonaws.com"
    },
```

```
    "eventTime": "2026-01-15T11:18:36Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "resiliencehub.amazonaws.com",
    "userAgent": "resiliencehub.amazonaws.com",
    "requestParameters": {
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionContext": {
            "aws:resiliencehub:service-arn": "arn:aws:resiliencehub:us-
west-2:111122223333:service/my-service:abc123",
            "aws-crypto-public-key": "AwAnnorjRE
+DFQYIuDKjGEvlXwro5Rdiegk8flmq7m0N..."
        }
    },
    "responseElements": null,
    "requestID": "c5bedc9b-e6d6-45f8-b121-c9851a3d718a",
    "eventID": "e839a7ed-e4a9-32a3-b92a-2c7237a40c82",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

当您通过 API 操作检索资源或评估工作流程处理先前存储的数据时，下一代 Resilience Hub 会发送解密数据的`Decrypt`请求。

以下示例事件记录了 `Decrypt` 操作：

```
{
    "eventVersion": "1.11",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLE:session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/YourRole/session-name",
        "accountId": "111122223333",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/YourRole",
                "accountId": "111122223333",
                "userName": "YourRole"
            }
        },
        "invokedBy": "resiliencehub.amazonaws.com"
    },
    "eventTime": "2026-01-15T11:27:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "resiliencehub.amazonaws.com",
    "userAgent": "resiliencehub.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "encryptionContext": {
            "aws:resiliencehub:service-arn": "arn:aws:resiliencehub:us-
west-2:111122223333:service/my-service:abc123",
            "aws-crypto-public-key": "A/9P3BC05WjeQONZR1fBiEqWKEse/
Yk1lMxd2VIh2ED5..."
        }
    },
    "responseElements": null,
    "requestID": "30f8e9bc-4e0a-4359-8bc3-8278ef42c206",
    "eventID": "195ef070-c952-4c28-9883-29bca297a08c",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DescribeKey

下一代 Resilience Hub 会发送DescribeKey请求，以验证与您的服务关联的客户托管密钥是否存在于账户和区域中，并且是有效的对称加密密钥。

以下示例事件记录了 DescribeKey 操作：

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLE:session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/YourRole/session-name",
        "accountId": "111122223333",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/YourRole",
                "accountId": "111122223333",
                "userName": "YourRole"
            }
        },
        "invokedBy": "resiliencehub.amazonaws.com"
    },
    "eventTime": "2026-01-15T10:07:13Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "resiliencehub.amazonaws.com",
    "userAgent": "resiliencehub.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "e427932c-448b-49aa-88e1-b311c27ba753",
```

```
    "eventID": "48c596a5-83c7-4603-b0cf-be0ff2548623",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

了解详情

以下资源提供有关静态数据加密的更多信息。

- 有关 AWS Key Management Service 基本概念的更多信息，请参阅 《AWS Key Management Service 开发人员指南》。
- 有关安全最佳实践的更多信息 AWS Key Management Service，请参阅《AWS Key Management Service 开发人员指南》。

传输中加密

所有传输中的数据均使用 TLS 1.2 或更高版本进行加密，包括：

- 对下一代弹性中心终端节点的 API 调用
- Cross-service 通信（下一代弹性中心到拓扑服务，下一代弹性中心到亚马逊 Bedrock）
- Cross-account 凭据传递（传输 AWS KMS 前已加密）

VPC 端点

您可以为下一代弹性中心创建 VPC 终端节点，将您的 VPC 和服务之间的流量保持在 AWS 网络内，而无需穿越公共互联网。这 AWS PrivateLink 用于私有连接。

您可以使用 VPC 终端节点私下将您的 VPC 连接到下一代弹性中心，而无需流量穿越公共互联网。

CloudTrail 整合

下一代 Resilence Hub 与 AWS CloudTrail (CloudTrail) 集成以记录对该服务进行的所有 API 调用，包括来自下一代 Resilence Hub 控制台的调用以及对下一代 Resilence Hub API 的编程调用。

合规性注意事项

有关适用于下一代 Resilience Hub 的合规计划的信息，请参阅按合规性计划划分的范围内 AWS 服务。

数据留存

下表显示了下一代弹性中心存储的数据的保留期。

数据类型	保留
评估结果和失效模式调查结果	2 年
系统和服务事件日志	2 年
发现的资源	1 年 TTL
拓扑快照	2 年
依赖关系数据	启用时长 + 30 天回顾

生成式 AI 数据处理

故障模式评估使用亚马逊 Bedrock 进行 AI 推断。以下数据处理做法适用：

- 客户数据的处理方式与服务 AWS 区域 相同
- 数据不用于训练或改进基础模型
- 评估输入和输出存储在静态加密的下一代 Resilience S3 存储 Hub-owned 桶中
- 客户可以完全选择退出生成式 AI 功能

最低权限建议

请遵循以下建议，将最低权限原则应用于您的下一代 Resilience Hub 配置：

1. ExternalId 用于跨账户角色 — 跨账户信任策略中的`ExternalId`条件可防止混淆的代理攻击。
2. 使用组织 Service-Linked 角色 -尽可能避免手动设置跨账户角色。 Service-Linked 角色提供自动限定范围、可审计的访问权限。

监控下一代弹性中心

您可以使用亚马逊和亚马逊监控下一代弹性中心 CloudWatch AWS CloudTrail， EventBridge 以跟踪评估活动、检测问题和自动响应。

主题

- CloudWatch 指标参考
- CloudTrail 事件日志
- EventBridge 通知
- 为下一代 Resilience Hub 设置 CloudWatch 警报

CloudWatch 指标参考

失败模式评估成功完成后，下一代 Resilience Hub 会在`ResilienceHub`命名空间下向您账户的亚马逊 CloudWatch (CloudWatch) 发布政策可实现性指标。指标仅在评估完成后发布。如果尚未进行任何评估，或者评估未产生可实现性结果，则不报告任何指标。

您的服务的权限模型必须包含调用者角色，该角色`cloudwatch:PutMetricData`有权让下一代 Resilenity Hub 向您的账户发布指标。

评估指标

每次成功评估失效模式后，都会发布以下指标。每个具有评估结果的策略组件都会发布一个数据点。

指标	Dimensions	说明	值
`PolicyAchievable`	`Service`, `PolicyComponent=AvailabilitySlo`	您的可用性 SLO 目标是否可以实现。	1.0 或 0.0
`PolicyAchievable`	`Service`, `PolicyCom`	您的多可用区 RTO 和 RPO 目标是否可以实现。	1.0 或 0.0

指标	Dimensions	说明	值
	ponent=MultiAzRtoRpo		
PolicyAchievable	Service, PolicyComponent=MultiRegionRtoRpo	您的多区域 RTO 和 RPO 目标是否可以实现。	1.0 或 0.0

下表描述了指标维度。

维度	说明
Service	正在评估的服务的名称。
PolicyComponent	正在评估抗灾政策组成部分。可能的值：AvailabilitySlo 、MultiAzRtoRpo 、MultiRegionRtoRpo 。

> **Note**
>
> 仅发布评估得出可实现性结果的政策组成部分。

针对该指标创建警报时使用Minimum统计数据。A Minimum 为 0.0 表示至少有一项评估认为该政策在评估期间无法实现。

CloudTrail 事件日志

下一代 Resilience Hub 与 AWS CloudTrail (CloudTrail) 集成在一起。所有 API 调用均作为事件记录 CloudTrail，包括来自下一代 Resilenision Hub 控制台的调用以及对下一代 Resilence Hub API 的编程调用。

支持的下一代弹性中心活动

所有下一代 Resilence Hub API 操作均已登录 CloudTrail，包括以下内容。

类别	示例事件
系统	CreateSystem ，DeleteSystem ，GetSystem ，ListSystems
服务	CreateService ，UpdateService ，DeleteService ，ListServices
策略	CreateResiliencePolicy ，UpdateResiliencePolicy ，DeleteResiliencePolicy
评测	StartFailureModeAssessment ，GetFailureModeAssessment ，ListFailureModeFindings
Discovery	StartServiceTopologyDiscovery ，ListDependencies ，ClassifyDependency
弹性测试	CreateTest ，GetTest, ListTests ，UpdateTest ，DeleteTest ，StartTestRun ，StopTestRun ，GetTestRun ，ListTestRuns ，ListTestTemplates ，GetTestTemplate ，PutTestSources ，DeleteTestSources ，ListTestSources ，ListTestRunSources ，ListTestRunEvents ，ListResolvedTestRunTargetResources

示例 CloudTrail 事件

以下是 StartFailureModeAssessment API 调用的示例 CloudTrail 事件。

```
{
  "eventVersion": "1.08",
  "eventSource": "resiliencehub.amazonaws.com",
  "eventName": "StartFailureModeAssessment",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.1",
  "userAgent": "aws-cli/2.x",
  "requestParameters": {
    "serviceArn": "arn:aws:resiliencehub:us-east-1:123456789012:service/
checkout:abc123"
```

```
  },
  "responseElements": {
    "assessmentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "status": "PENDING"
  }
}
```

EventBridge 通知

借助 Amazon EventBridge，您可以使用事件驱动的规则监控下一代 Resilience Hub 中的资源。这些规则可以触发其他 AWS 服务中的操作。例如，您可以创建一条规则，每当故障模式评估完成或发现新的依赖关系时，都会向 Amazon SNS 主题发出信号。

您可以在中创建规则 EventBridge ，对下一代 Resilience Hub 中的以下事件采取行动：

- 失效模式评估已完成 -失效模式评估成功完成时发出。
- 失效模式评估失败 -失效模式评估工作流程失败时发出。
- 故障模式评估已排队 -当评估排队等待延迟处理时发出。评估将在 24 小时内重试。
- 失效模式查找结果已解决 -当故障模式查找结果标记为 “已解决” 或 “不相关” 时发出。
- 发现了新的依赖关系 -当依赖项发现为您的服务确定了新的依赖关系时发出。

要捕获您感兴趣的下一代 Resilience Hub 中的特定事件，请定义 EventBridge 可用于检测事件的特定事件模式。事件规律与它们匹配的事件具有相同的结构。模式引用了您要匹配的字段，并提供您所查找的值。

下一代 Resilience Hub 会尽最大努力发出事件，并在服务正常 EventBridge运行时近乎实时地将其交付给。但是，某些情况可能会延迟或阻止事件传送。

有关 EventBridge 规则和事件模式的更多信息，请参阅中的事件和事件模式 EventBridge。

为下一代 Resilience Hub 的事件创建 EventBridge 规则

使用 EventBridge，您可以创建规则，定义下一代 Resilence Hub 为您的服务发出事件时应采取的操作。

下一代 Resilience Hub 使用源`aws.resiliencehub`发出所有事件。您的事件模式必须包含此来源，才能匹配来自下一代 Resilience Hub 的事件。您可以进一步筛选`detail-type`以匹配特定的事件类型。

要将事件模式输入或粘贴到 EventBridge 控制台中，请选择 Enter my own 选项。为了帮助您确定可能有用的事件模式，本主题包括事件模式和事件示例。

为下一代 Resilience Hub 的事件创建规则

1. 在处打开 EventBridge 控制台https://console.aws.amazon.com/events/。
2. 为此 AWS 区域，选择您在下一代 Resilience Hub 中部署服务的区域。
3. 选择 Create rule (创建规则)。
4. 输入规则的 Name (名称) 和“Description (描述)”（可选）。
5. 对于事件总线，保留默认值，即默认。
6. 选择下一步。
7. 对于事件源，保留默认值，即 AWS 事件。
8. 在 “活动模式” 下，选择 “输入我自己的模式” 。
9. 输入或粘贴包含`"source": ["aws.resiliencehub"]`和`detail-type`要匹配的事件模式。有关示例，请参阅 事件模式和事件示例。
10. 选择下一步并配置您的目标（例如，Amazon SNS 主题、Lambda 函数或 CloudWatch 日志组）。
11. 选择创建规则，完成规则创建工作流程。

事件模式和事件示例

事件规律与它们匹配的事件具有相同的结构。模式引用了您要匹配的字段，并提供您所查找的值。

您可以将本部分中的事件模式复制并粘贴到中， EventBridge 以创建监控下一代 Resilence Hub 事件的规则。

选择所有失效模式评估完成事件

以下模式与所有已完成的评估相匹配。

```
{
  "source": ["aws.resiliencehub"],
  "detail-type": ["Failure Mode Assessment Completed"]
}
```

选择所有失效模式评估失败事件

以下模式与所有失败的评估相匹配。

```
{
  "source": ["aws.resiliencehub"],
  "detail-type": ["Failure Mode Assessment Failed"]
}
```

选择所有新发现的依赖项事件

以下模式匹配所有新的依赖事件。

```
{
  "source": ["aws.resiliencehub"],
  "detail-type": ["New Dependency Discovered"]
}
```

从下一代 Resilience Hub 中选择所有活动

以下模式匹配所有事件，无论类型如何。

```
{
  "source": ["aws.resiliencehub"]
}
```

选择具有高严重性发现的评估事件

以下模式与确定至少一项高严重性发现的评估相匹配。

```
{
  "source": ["aws.resiliencehub"],
  "detail-type": ["Failure Mode Assessment Completed"],
  "detail": {
    "highSeverityCount": [{"numeric": [">", 0]}]
  }
}
```

以下部分提供了每种事件类型的示例事件。

故障模式评估已完成事件

以下是失效模式评估成功完成时触发的示例事件。

```
{
  "version": "0",
```

```
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Failure Mode Assessment Completed",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "assessmentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "status": "SUCCESS",
    "findingsCount": 5,
    "highSeverityCount": 2
  }
}
```

detail 对象包含以下字段：

字段	说明
assessmentId	已完成评估的唯一标识符。
status	评估状态。价值：SUCCESS。
findingsCount	已识别的故障模式发现的总数。
highSeverityCount	已确定的高严重性发现的数量。

失败模式评估失败事件

以下是失效模式评估失败时触发的示例事件。

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Failure Mode Assessment Failed",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
```

```
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "assessmentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "status": "FAILED",
    "failureReason": "Unable to assume the invoker role specified in the service
 configuration."
  }
}
```

detail 对象包含以下字段：

字段	说明
assessmentId	失败评估的唯一标识符。
status	评估状态。价值：FAILED。
failureReason	对评估失败原因的描述。

故障模式评估队列事件

以下是评估排队等待延迟处理时触发的示例事件。评估将重试并在 24 小时内完成。

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Failure Mode Assessment Queued",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "assessmentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
  }
}
```

detail 对象包含以下字段：

字段	说明
assessmentId	排队评估的唯一标识符。

排队的评估完成后，将发出单独的Failure Mode Assessment Completed或Failure Mode Assessment Failed事件。

失败模式查找已解决的事件

以下是将失效模式查找结果标记为 “已解决” 或 “不相关” 时触发的示例事件。

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Failure Mode Finding Resolved",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "findingId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "status": "RESOLVED",
    "severity": "HIGH",
    "category": "SINGLE_POINT_OF_FAILURE"
  }
}
```

detail 对象包含以下字段：

字段	说明
findingId	已解析结果的唯一标识符。
status	分辨率状态。价值观：RESOLVED，IRRELEVANT 。
severity	调查结果的严重性。值：HIGH、MEDIUM、LOW。

字段	说明
category	失效模式类别（例如，SINGLE_POINT_OF_FAILURE ，SHARED_FATE ）。

新的依赖关系发现事件

以下是依赖项发现为您的服务确定新的依赖项时触发的示例事件。此事件在稳定周期后发出，以减少初始发现期间的噪音。

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "New Dependency Discovered",
  "source": "aws.resiliencehub",
  "account": "111122223333",
  "time": "2026-01-15T10:30:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resiliencehub:us-east-1:111122223333:service/my-service:abc123"
  ],
  "detail": {
    "dependencyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "dependencyName": "S3",
    "dnsName": "s3.us-east-1.amazonaws.com.",
    "location": "us-east-1",
    "provider": "AWS",
    "sourceRegions": [
      "us-east-1",
      "us-west-2"
    ]
  }
}
```

detail 对象包含以下字段：

字段	说明
dependencyId	已发现依赖项的唯一标识符。

字段	说明
dependencyName	依赖关系的名称（例如，AWS 服务名称）。
dnsName	您的服务用于与依赖项通信的 DNS 名称。
location	托管依赖项的 AWS 区域 或位置。
provider	依赖关系提供者。值包括AWS、ThirdPart y 、Internal。
sourceRegions	您的服务与该依赖项进行通信的区域。

为下一代 Resilience Hub 设置 CloudWatch 警报

您可以根据下一代 Resilience Hub 指标创建 CloudWatch 警报，以便在无法实现弹性策略时收到通知。

警报：政策无法实现

以下示例创建了一个警报，该警报在名为的服务无法实现可用性 SLO 策略时触发。my-service

```
aws cloudwatch put-metric-alarm \
  --alarm-name "ResilienceHub-PolicyNotAchievable-AvailabilitySlo" \
  --metric-name "PolicyAchievable" \
  --namespace "ResilienceHub" \
  --dimensions Name=Service,Value=my-service Name=PolicyComponent,Value=AvailabilitySlo
 \
  --statistic Minimum \
  --period 86400 \
  --threshold 1 \
  --comparison-operator LessThanThreshold \
  --evaluation-periods 1 \
  --treat-missing-data notBreaching \
  --alarm-actions "arn:aws:sns:us-east-1:123456789012:resilience-hub-alerts"
```

当评估期内的任何评估报告无法实现该政策（指标值 0.0）时，此警报即进入ALARM状态。该--treat-missing-data notBreaching设置可确保在没有数据点的情况下不会在两次评估之间触发警报。

限额和限制

您的 AWS 账户对每项 AWS 服务都有默认配额，以前称为限额。除非另有说明，否则每个配额都是 AWS 区域特定的。您可以申请增加某些配额，而不能增加其他配额。

服务配额

下表列出了下一代弹性中心的配额。

#	资源	默认配额	可调整
1	每个账户的系统数 AWS 区域	500	是
2	每个账户的服务量 AWS 区域	100	是
3	每个系统的用户旅程	20	否
4	每项服务的应评估资源	500	是
5	每项服务的资源总量	2000	否
6	每项服务的输入源	20	是
7	每项服务的服务功能	20	否
8	每个账户的弹性政策 AWS 区域	100	否
9	每月包括每项服务的故障模式评估	2	否
10	跟踪每项服务的依赖关系	10000	否
11	Cross-account 每个服务的角色 ARN	5	否
12	每项服务的服务指标	10	否
13	对每项服务进行主动测试	1	否
14	每次测试的测试来源	5	否
15	每个测试模板的测试	1	否

弹性测试正在运行 AWS Fault Injection Service，因此 AWS FIS 服务配额也适用于您的测试运行。其中包括最大活跃实验次数和最长动作持续时间的配额。有关更多信息，请参阅的配额和限制 AWS Fault Injection Service。

硬限制

以下配额不能提高。

#	资源	硬限制
1	每个账户的系统数 AWS 区域 （最大）	1000
2	每项服务的输入源（最大值）	100
3	每项服务的资源（最大）	1000
4	每个系统的用户旅程（最大）	100
5	Cross-account 每个服务的角色 ARN	5
6	每月包括每项服务的故障模式评估	2

申请增加配额

您可以使用服务配额控制台或联系 AWS 支持部门申请增加可调整配额。

要使用服务配额申请增加配额，请执行以下操作：

1. 打开服务限额控制台。
2. 在导航窗格中，选择 AWS 服务。
3. 选择 “AWS 弹性中心” 。
4. 选择要增加的配额。
5. 选择请求增加限额。
6. 输入新的限额值，然后选择请求。

要通过 AWS 支持申请增加配额，请执行以下操作：

1. 打开AWS 支持中心。

2. 选择创建工单。
3. 选择增加服务限制。
4. 选择 R esilien ce Hub 作为服务。
5. 填写所需信息并提交您的请求。

配额增加请求通常会在几个工作日内处理。

对下一代弹性中心进行故障排除

本节为您在使用下一代 Resilience Hub 时可能遇到的常见问题提供解决方案。

主题

- 依赖关系发现问题
- 失效模式评估问题
- IAM 和权限错误
- AWS 组织配置问题
- 资源发现问题
- 弹性测试问题
- 已知问题和变通方法

依赖关系发现问题

以下是与依赖关系发现相关的常见问题。

发现未返回预期的依赖关系

症状：您启用了依赖项发现，但看不到已知存在的依赖关系。

下表列出了可能的原因和解决方案。

原因	解决方案
依赖关系使用直接 IP（不是 DNS）	依赖关系发现依赖于 DNS 查询。未发现通过 IP 地址建立的连接。手动跟踪 IP-based 依赖关系。

原因	解决方案
计算资源不在 VPC 中	Non-VPC Lambda 函数不生成 Route 53 解析器查询。将 Lambda 连接到 VPC 或手动跟踪依赖关系。
在 35 天期限内未调用依赖关系	必须在 35 天回顾期内调用依赖关系。很少出现的呼叫可能不会出现。
通过非 Route 53 解析器解析 DNS	自定义 DNS 解析器绕过 Route 53 查询日志。确保您的 VPC 使用默认的 Route 53 解析器。

Kubernetes 归因差距

症状：已发现依赖关系，但归因于共享 EKS 集群中的错误服务。

原因：当多个服务共享一个 EKS 集群时，DNS 查询归因于节点级别，而不是 pod 级别。

解决方案：增强的 pod 级别归因计划在未来的版本中发布。目前，手动查看共享集群的依赖关系。

Non-VPC Lambda 没有出现

症状：未发现 Lambda 函数依赖关系。

原因：未连接到 VPC 的 Lambda 函数不通过 Route 53 解析器进行 DNS 查询。

解决方案：要么将 Lambda 函数连接到 VPC，要么在 Resilience Hub 之外手动跟踪其依赖关系。

失效模式评估问题

以下是与故障模式评估相关的常见问题。

评估未完成

症状：评估处于`IN_PROGRESS`状态的时间超过 30 分钟。

下表列出了可能的原因和解决方案。

原因	解决方案
大型服务（大量资源）	对拥有 1,000 或更多资源的服务进行评估可能需要更长时间。等待最多 60 分钟。

原因	解决方案
调用者角色权限问题	验证调用者角色是否已附加ReadOnlyAccess 。AWSResilienceHubV2AssessmentExecutionPolicy
拓扑未完成	在开始评估之前，请确保成功StartServiceTopologyDiscovery 完成。
服务错误	如果评估失败，请检查GetFailureModeAssessment 响应中的错误消息。

评估因未找到拓扑而失败

症状：StartFailureModeAssessment返回有关缺少拓扑的错误。

解决方案：**StartServiceTopologyDiscovery**先运行并等待成功完成。评估需要完整的拓扑。

故障模式调查结果与预期策略不符

症状：评估失败模式的发现似乎与您应用的策略无关。

可能的原因：

- 评估运行后应用了策略 — 重新进行评估。
- 适用多种政策（从用户旅程和服务级别来看）——查看所有适用的政策。
- 失效模式的发现与 Well-Architected 最佳实践有关，而不是特定的政策要求。

评估未得出故障模式结果

症状：评估成功完成，但返回的故障模式结果为零。

可能的原因：

- 服务资源很少（评估需要足够的架构来分析）。
- 不应用任何政策（没有政策的评估产生的结果较少）。
- 架构已经满足所有要求。

IAM 和权限错误

以下是常见的 IAM 和权限错误。

常见权限错误代码和解决方法

下表列出了常见的权限错误代码及其推荐的解决方案。

错误	原因	解决方案
`AccessDeniedException: Unable to assume role`	调用者角色信任政策不包括 `resiliencehub.amazonaws.com`	更新角色的信任政策。
`AccessDeniedException: Cross-account role`	Cross-account 角色信任策略不允许从调用者角色中进行假设	验证信任政策，然后 `ExternalId` 。
`AccessDeniedException: sts:AssumeRole`	调用者角色缺乏跨账户角色的`sts:AssumeRole` 权限	为调用者角色添加`sts:AssumeRole` 权限。
`InvalidParameterException: Role does not exist`	中的角色名称与现有 IAM 角色`permissionModel` 不匹配	验证角色名称和账户。

验证角色配置

使用以下 AWS CLI 命令检查您的调用者角色是否配置正确。

要验证角色是否存在，请执行以下操作：

```
aws iam get-role --role-name AWSResilienceHubAssessmentRole
```

要验证信任策略，请执行以下操作：

```
aws iam get-role --role-name AWSResilienceHubAssessmentRole \
  --query 'Role.AssumeRolePolicyDocument'
```

要模拟校长能否执行所需的操作，请执行以下操作：

```
aws iam simulate-principal-policy \
  --policy-source-arn arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole \
  --action-names resiliencehub:GetService resiliencehub:StartFailureModeAssessment
```

AWS 组织配置问题

以下是常见 AWS 的组织配置问题。

委派管理员设置错误

错误	原因	解决方案
`AWSOrganizationsNotInUseException`	组织未启用	为 AWS 组织启用所有功能。
`AccountNotRegisteredException`	账户不是该组织的成员	验证账户成员资格。
`ConstraintViolationException`	未启用服务信任	`enable-aws-service-access` 先跑。

会员账户知名度差距

症状：委派管理员无法看到成员账户中的服务。

下表列出了可能的原因和解决方案。

原因	解决方案
Service-linked 角色尚未创建	对于大型组织而言，创建服务相关角色可能需要时间。等着再检查一遍。
账户在设置期间被暂停	取消暂停该账户。12 小时协调任务将创建服务相关角色。
账户最近加入组织	新账户会自动获得服务相关角色，但可能会有短暂的延迟。

原因	解决方案
服务信任已禁用	Re-enable 来自管理账户的可信访问权限。

验证成员账户中是否存在服务相关角色

在成员账户中运行以下命令以验证服务相关角色是否存在：

```
aws iam get-role --role-name AWSServiceRoleForResilienceHub
```

如果角色不存在，请验证可信访问权限是否已启用，然后等待协调任务，该任务每 12 小时运行一次。

资源发现问题

以下是常见的资源发现问题。

CloudFormation 未找到堆栈

症状：资源发现失败并显示 “未找到堆栈”。

解决方案

- 验证堆栈 ARN 是否正确且堆栈存在。
- 验证调用者角色是否具有`cloudformation:DescribeStackResources`权限。
- 对于跨账户堆栈，请验证跨账户角色是否具有访问权限。

Terraform 状态文件无法访问

症状：资源发现无法读取 Terraform 状态文件。

解决方案

- 验证 Amazon S3 存储桶和密钥路径是否正确。
- 验证调用者角色对状态`s3:GetObject`文件具有权限。
- 验证状态文件是否采用支持的格式。

已发现资源但拓扑生成失败

症状：资源出现在列表中，但拓扑显示没有连接。

解决方案

- 验证调用者角色是否具备`ReadOnlyAccess`（拓扑查询必需）。
- 检查资源是否在 VPC 中（拓扑生成地图 VPC-based连接）。
- 对于 EKS 资源，请验证 Kubernetes RBAC 是否已配置。

不支持和排除的资源类型

下一代 Resilience Hub 将某些资源类型排除在发现范围之外，因为它们没有独立的弹性价值。如果您期望某个资源出现在已发现的资源中但事实并非如此，则该资源可能属于排除类型。

从未发现过资源类型

下一代 Resilience Hub 在发现期间从不存储以下资源类型。这些资源类型包括辅助基础架构、时间点备份和与弹性分析无关的操作工具。

资源类型
AWS::EC2::EIP
AWS::EC2::Volume
AWS::EC2::Snapshot
AWS::FSx::Snapshot
AWS::Lightsail::DiskSnapshot
AWS::RDS::DBSnapshot
AWS::RDS::DBClusterSnapshot
AWS::EC2::FlowLog
AWS::CloudWatch::Dashboard
AWS::Logs::LogGroup

资源类型
AWS::Logs::MetricFilter
AWS::SSM::ResourceDataSync
AWS::RDS::DBParameterGroup
AWS::RDS::DBClusterParameterGroup
AWS::ElastiCache::ParameterGroup
AWS::RDS::DBSubnetGroup
AWS::ElastiCache::SubnetGroup
AWS::EC2::SubnetNetworkAclAssociation
AWS::EC2::VPCGatewayAttachment
AWS::CloudFormation::Stack
AWS::CloudFormation::WaitConditionHandle
AWS::CodeDeploy::DeploymentGroup
AWS::KMS::Alias
AWS::SecretsManager::SecretTargetAttachment
AWS::CloudFormation::CustomResource

已存储但未计费的资源类型

下一代 Resilience Hub 会发现并存储以下资源类型以供参考，但不会将其计入您的计费资源配额。它们没有出现在弹性分析中。

资源类型
AWS::IAM::Role

资源类型
AWS::IAM::Policy
AWS::IAM::ManagedPolicy
AWS::IAM::InstanceProfile
AWS::Lambda::LayerVersion
AWS::Lambda::Permission
AWS::EC2::LaunchTemplate
AWS::EC2::SecurityGroup
AWS::EC2::SubnetRouteTableAssociation
AWS::CloudFront::OriginRequestPolicy
AWS::CloudFront::CloudFrontOriginAccessIdentity
AWS::SecretsManager::Secret
AWS::CloudWatch::Alarm
AWS::CDK::Metadata

已发现资源和拓扑资源之间的区别

您在 ListResources API 响应中看到的资源可能比拓扑图中显示的资源还要多。并非所有发现的资源都显示在拓扑视图中。拓扑是显示资源如何交互的连接图。下一代 Resilience Hub 将与其他资源没有连接的资源从拓扑视图中移除。

EC2 实例或 ECS 任务未显示为应计费资源

当父资源（例如 Auto Scaling 组、ECS 服务或 EKS 部署）管理 EC2 实例、ECS 任务、 EKS 容器或网络接口时，下一代弹性中心会将该资源归类为临时资源。临时资源是短暂的。父资源通过生命周期事件自动替换它们。下一代韧性中心通过他们的父母而不是独立地对他们进行评估。

当由父级管理时，以下资源类型是短暂的：

资源类型	家长示例
AWS::EC2::Instance	Auto Scaling 组或 EKS 节点组
AWS::ECS::Task	ECS 服务
AWS::EKS::Pod	EKS 部署或副本集
AWS::EC2::NetworkInterface	由 Auto Scaling 管理的 EC2 实例

这些类型的独立实例（不由父实例管理）仍可计费。

弹性测试问题

以下是与弹性测试相关的常见问题。

测试运行无法启动

症状：开始测试运行会返回 a ConflictException。

原因：下一代 Resilience Hub 一次只能对目标运行一次测试。该服务的上一次运行仍在进行中。

解决方案：等待当前运行完成，或停止运行StopTestRun，然后开始新的运行。

测试运行因访问被拒绝错误而失败

症状：由于来自目标服务 AWS FIS 或其中一个目标服务的AccessDenied错误，测试运行失败。

下表列出了可能的原因和解决方案。

原因	解决方案
执行角色信任策略不允许 AWS FIS	验证角色信任fis.amazonaws.com 以及和aws:SourceArn 条件是否与您的账户相匹配。aws:SourceAccount 有关信任政策，请参阅用于弹性测试的 IAM 执行角色。
执行角色缺少测试模板的权限	每个测试模板运行一组不同的 AWS FIS 操作。为正在运行的模板附加权限策略。有关政策，请参阅用于弹性测试的 IAM 执行角色。

原因	解决方案
Multi-account 未配置角色链	对于多账户测试，请验证协调器角色可以在包含目标资源的每个账户中代入目标角色。

测试运行在完成之前停止

症状：测试运行在完成之前会自行停止。

原因：您配置为停止条件的 CloudWatch 警报超过了其阈值，弹性测试停止了运行以限制影响。

解决方案：查看触发停止条件的警报，以确定对您的服务的影响。解决潜在问题后，开始新的测试运行。

跳过所有操作后，测试运行完成

症状：测试运行已完成，但未注入任何故障。显示所有动作`skipped`。

原因：在所选可用区或区域中，没有任何资源与任何操作的目标资源类型相匹配。

解决方案：验证资源发现已完成且您选择了正确的可用区或区域。

依赖关系错误操作因设置错误而失败

症状：由于未配置所需的代理或 sidecar，依赖关系错误操作失败。

原因：丢包操作需要 Amazon EC2 上的 SSM 代理、亚马逊 ECS 任务定义中的 SSM 容器或亚马逊 EKS 容器的 Kubernetes 服务账户。

解决方案：按照AWS FIS 操作参考中针对您的计算类型的设置步骤进行操作。

并非所有依赖项都在测试中可见

症状：并非所有已发现的依赖项都显示在下拉列表中。

原因：按测试筛选依赖关系，仅显示与测试范围相关的依赖关系。

解决方案：每个测试显示不同的子集。请参阅显示依赖关系的各个测试页面。

已知问题和变通方法

本节列出了下一代 Resilience Hub 中的已知问题及其推荐的解决方法。有关最新信息，请参阅下一代 Resilience Hub 发行说明。

API 参考

本节按功能区概述了下一代弹性中心API操作。有关包括请求和响应架构在内的完整 API 规范，请参阅下一代 Resilience Hub API 参考。

主题

- 发出 API 请求和身份验证
- 操作
- 数据类型
- 错误代码

发出 API 请求和身份验证

Endpoint

```
https://resiliencehub.{region}.amazonaws.com
```

API 版本

下一代 Resilience Hub API 使用/v3路径前缀。所有请求都必须使用 AWS 签名版本 4 (SigV4) 进行签名。

身份验证

所有 API 调用都需要有效的 AWS 证书。下一代弹性中心使用 AWS IAM 进行授权。确保您的 IAM 政策允许resiliencehub:*采取必要的行动。

操作

下一代弹性中心 API 提供以下类别的操作。

复原力政策

处理建议	方法	说明
CreatePolicy	POST	使用可用性 SLO、 RTO/RPO 目标和灾难恢复方法创建弹性策略。

处理建议	方法	说明
UpdatePolicy	POST	更新策略目标和配置。
GetPolicy	GET	检索政策详情。
ListPolicies	GET	列出具有相关服务数量的策略。
DeletePolicy	POST	删除策略。

系统

处理建议	方法	说明
CreateSystem	POST	创建支持可选依赖项发现的系统。
UpdateSystem	POST	更新系统描述、依赖关系发现和 KMS 密钥。
GetSystem	GET	检索系统详细信息。
ListSystems	GET	列出系统，可按organizationId ouId、和accountId 筛选。
DeleteSystem	POST	删除系统（必须没有关联服务）。

用户旅程

处理建议	方法	说明
CreateUserJourney	POST	在系统下创建用户旅程。
UpdateUserJourney	POST	更新用户旅程服务和政策。
GetUserJourney	GET	检索用户旅程详情。
ListUserJourneys	GET	列出系统的用户旅程。
DeleteUserJourney	POST	删除用户旅程。

服务

处理建议	方法	说明
CreateService	POST	使用区域、权限模型、报告配置和依赖关系发现设置创建服务。
UpdateService	POST	更新服务配置，包括权限模型和依赖关系发现。
GetService	GET	检索完整的服务详细信息，包括有效的保单价值和弹性分数。
ListServices	GET	列出服务，可按systemId、、、userJourneyId 、organizationId ouIdaccountId assessmentStatus 、和policyArn 进行筛选。
DeleteService	POST	删除服务。

输入源

处理建议	方法	说明
CreateInputSource	POST	配置资源发现源（资源标签、 CloudFormation 堆栈、Terraform 状态文件、EKS 集群或设计文件）。对于具有多个标签的基于标签的单一输入源，该服务仅发现与所有指定标签匹配的资源。对于多个基于标签的输入源，该服务会发现与其中任何一个输入源匹配的资源。
ListInputSources	GET	列出服务的输入源。
DeleteInputSource	POST	删除输入源。

资源

处理建议	方法	说明
ListResources	GET	列出已发现的服务资源，可按serviceFunctionId 和awsRegion 筛选。

失效模式评估

处理建议	方法	说明
StartFailureModeAssessment	POST	触发异步 AI-powered 评估，以创建拓扑、服务功能和故障模式调查结果。
ListFailureModeAssessments	GET	列出包含状态、弹性分数和报告信息的评估。

弹性测试

处理建议	方法	说明
ListTestTemplates	GET	列出可用的测试模板。
GetTestTemplate	GET	检索测试模板，包括其操作和参数。
CreateTest	POST	使用测试模板为服务创建测试。
GetTest	GET	检索包括参数、停止条件和角色的测试配置。
UpdateTest	POST	更新测试配置，包括参数、停止条件和角色。
ListTests	GET	列出服务的测试。
DeleteTest	POST	删除测试。
StartTestRun	POST	开始测试服务。

处理建议	方法	说明
StopTestRun	POST	停止测试运行。
ListTestRuns	GET	列出服务的测试运行次数。
GetTestRun	GET	检索包括状态、参数和时间戳在内的测试运行。
ListTestRunEvents	GET	列出测试运行时间表中的事件。
PutTestSources	POST	为测试添加或更新成功标准警报或可观测性警报。
DeleteTestSources	POST	从测试中移除成功标准警报或可观察性警报。
ListTestSources	GET	列出测试的成功标准警报或可观察性警报。
ListTestRunSources	GET	列出测试运行的成功标准警报或可观测性警报。
ListResolvedTestRunTargetResources	GET	列出已解析为试运行目标的资源。

拓扑

处理建议	方法	说明
ListServiceTopologyEdges	GET	列出服务的资源依赖边缘。

服务功能

处理建议	方法	说明
CreateServiceFunction	POST	创建具有重要性 (PRIMARY/SUPPLEMENTAL) 的服务函数。
UpdateServiceFunction	POST	更新服务功能属性。

处理建议	方法	说明
ListServiceFunctions	GET	列出服务的服务函数。
DeleteServiceFunction	POST	删除服务函数。
AddServiceFunctionResources	POST	将资源与服务功能相关联（每次调用最多 10 个）。
DeleteServiceFunctionResources	POST	删除资源关联（每次调用最多 10 个）。

失效模式调查结果

处理建议	方法	说明
GetFailureModeFinding	GET	检索故障模式查找详细信息，包括 AI-generated建议。
UpdateFailureModeFinding	POST	更新失败模式查找状态（已解决，不相关）并添加注释。
ListFailureModeFindings	GET	列出故障模式调查结果，可按severityfailureCategory 、和status进行筛选。

断言

处理建议	方法	说明
CreateAssertion	POST	使用类别和文本创建弹性断言。
UpdateAssertion	POST	更新断言文本或类别。
ListAssertions	GET	列出断言，可按类别和来源（USER或SYSTEM）过滤。

处理建议	方法	说明
DeleteAssertion	POST	删除断言。

依赖项

处理建议	方法	说明
UpdateDependency	POST	更新依赖项元数据（注释、重要性分类）。
ListDependencies	GET	列出已发现的服务依赖关系。

Reports

处理建议	方法	说明
CreateReport	POST	生成 PDF 报告（FAILURE_MODE DEPENDENCY 、或TESTING键入）；写入客户的 Amazon S3 存储桶。
ListReports	GET	列出包含状态和 Amazon S3 输出位置的生成的报告。

Events

处理建议	方法	说明
ListServiceEvents	GET	列出服务的审计事件（包括 actor:USER/SYSTEM、分数变化）。
ListSystemEvents	GET	列出系统的审计事件。

迁移

处理建议	方法	说明
ImportApp	POST	将 v1 Resilience Hub 应用程序导入 v2 服务。
ImportPolicy	POST	将 v1 策略导入 v2 格式。

数据类型

下表列出了下一代 Resilience Hub API 使用的关键数据类型。

Type	说明
SystemEntity	包含 ARN、名称、描述和创建时间的系统。
UserJourneyEntity	包含名称、描述、服务列表和政策的用户旅程。
ServiceEntity	包含 ARN、名称、系统关联、权限模型和输入源的服务。
ResiliencePolicyEntity	包含名称和组件（灾难恢复、可用性、性能）的策略。
AssessmentEntity	使用 ID、状态、时间戳和失效模式的评估结果很重要。
FindingEntity	使用 ID、名称、描述、严重程度和建议进行故障模式查找。
RecommendationEntity	包含名称、描述、成本和复杂性的建议。
DependencyDiscoveryConfig	包含状态、符合条件的资源数、消息和上次更新的时间戳的依赖关系发现配置。由GetService 和返回ListServices 。
DependencyEntity	具有名称、位置、重要程度和允许状态的依赖关系。
TopologyEntity	包含 ID、时间戳、资源数和边的拓扑。

DependencyDiscoveryConfig 结构

```
{
  "status": "INITIALIZING | ENABLED | DISABLED",
  "updatedAt": "timestamp",
  "eligibleResourceCount": integer,
  "message": "string"
}
```

下表描述了DependencyDiscoveryConfig结构中的字段。

字段	必填	描述
status	是	依赖关系发现的当前状态。有效值：INITIALIZING （发现正在运行）、ENABLED（发现已完成且处于活动状态）或DISABLED（发现已关闭）。
updatedAt	否	上次更新依赖项发现状态的时间戳。
eligibleResourceCount	否	符合依赖关系发现条件的计算资源的数量。在资源发现过程完成首次运行null之前返回。
message	否	描述当前发现状态的消息。null当发现完成且依赖关系可用时返回。

权限模型结构

```
{
  "invokerRoleName": "string",
  "crossAccountRoles": [
    {
      "crossAccountRoleArn": "string",
      "externalId": "string"
    }
  ]
}
```

策略组件结构

```
{
  "multiRegionDr": {
    "required": "boolean",
    "rtoMinutes": "integer",
    "rpoMinutes": "integer"
  },
  "availabilitySlo": {
    "targetPercentage": "number",
    "performanceConditions": {
      "expression": "string",
      "conditions": [
        {
          "type": "FAULT_RATE | LATENCY | VOLUME",
          "operator": "LESS_THAN | GREATER_THAN",
          "value": "number",
          "percentile": "string"
        }
      ]
    }
  },
  "dataProtection": {
    "rpoMinutes": "integer"
  }
}
```

错误代码

下表列出了下一代 Resilience Hub API 返回的错误代码。

错误代码	HTTP 状态	说明
ValidationException	400	请求参数无效。
ResourceNotFoundException	404	指定的资源不存在。
ConflictException	409	操作与当前状态冲突（例如，评估已在运行）。
AccessDeniedException	403	来电者缺乏所需的权限。

错误代码	HTTP 状态	说明
ThrottlingException	429	超出请求速率。
InternalServerException	500	内部服务错误。
ServiceQuotaExceededException	402	已超过服务配额。

常见错误场景

场景	错误	解决方案
在没有拓扑的情况下开始评估	ConflictException	StartServiceTopologyDiscovery 先跑。
在运行时开始评估	ConflictException	等待当前评估完成。
使用服务删除系统	ConflictException	首先移除所有服务关联。
Cross-account 无需角色即可访问	AccessDeniedException	配置跨账户角色或启用组织。
超过 5 个跨账户角色	ServiceQuotaExceededException	使用 AWS 组织进行更大规模的部署。

下一代 Resilence Hub 用户指南的文档历史记录

下表描述了下一代 Resilience Hub 的文档版本。

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》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。