Benutzerhandbuch

AWS Zentrum für Resilienz

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

AWS Zentrum für Resilienz: Benutzerhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Resilience Hub?

AWS Resilience Hub ist ein zentraler Ort, an dem Sie die Ausfallsicherheit Ihrer Anwendungen verwalten und verbessern können. AWS AWS Resilience Hub ermöglicht es Ihnen, Ihre Resilienzziele zu definieren, Ihre Resilienzsituation anhand dieser Ziele zu bewerten und Verbesserungsempfehlungen auf der Grundlage des AWS Well-Architected Framework umzusetzen. Darin AWS Resilience Hub können Sie auch Amazon Fault Injection Service-Experimente erstellen und ausführen, die reale Störungen Ihrer Anwendung nachahmen, sodass Sie Abhängigkeiten besser verstehen und potenzielle Schwächen aufdecken können. AWS Resilience Hub bietet einen zentralen Ort mit allen AWS Services und Tools, die Sie benötigen, um Ihre Widerstandsfähigkeit kontinuierlich zu stärken. AWS Resilience Hub arbeitet mit anderen Diensten zusammen, um Empfehlungen zu geben und Sie bei der Verwaltung Ihrer Anwendungsressourcen zu unterstützen. Weitere Informationen finden Sie unter Arbeiten mit anderen -Services.

Die folgende Tabelle enthält die Dokumentationslinks zu allen zugehörigen Resilienzdiensten.

Verwandte AWS Resilienzdienste und Referenzen

AWS Resilienz-Service	Link zur Dokumentation
AWS Elastic Disaster Recovery	Was ist Elastic Disaster Recovery
AWS Backup	Was ist AWS Backup
Amazon Route 53-Controller für die Anwendungswiederherstellung (Route 53ARC)	Was ist Amazon Route 53 Application Recovery Controller

Themen

- AWS Resilience Hub — Resilienzmanagement
- AWS Resilience Hub — Resilienztests
- AWS Resilience Hub Konzepte
- AWS Resilience Hub Personas
- AWS Resilience Hub unterstützte Ressourcen

AWS Resilience Hub — Resilienzmanagement

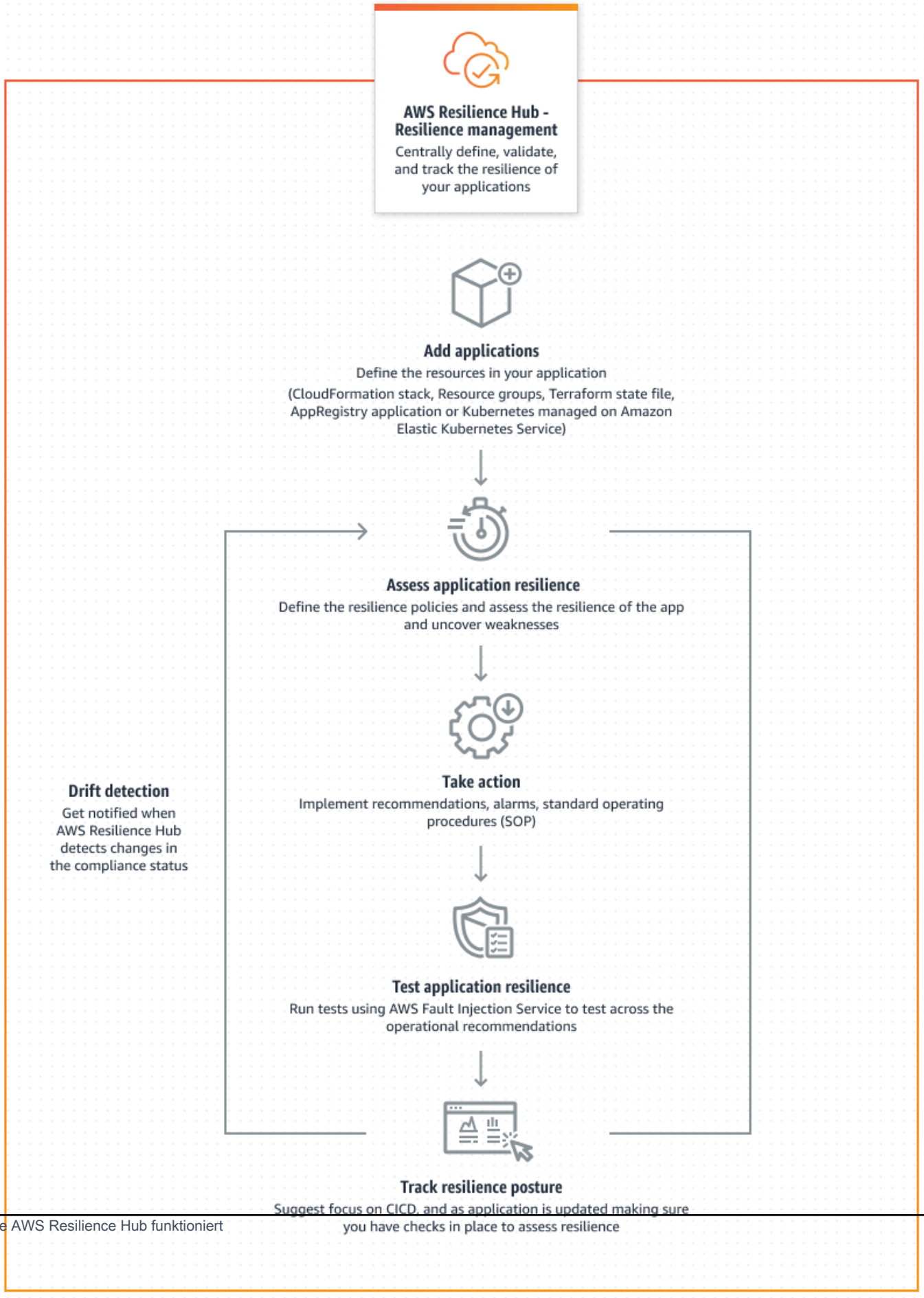
AWS Resilience Hub bietet Ihnen einen zentralen Ort, an dem Sie die Ausfallsicherheit Ihrer AWS Anwendung definieren, validieren und verfolgen können. AWS Resilience Hub hilft Ihnen dabei, Ihre Anwendungen vor Störungen zu schützen und die Wiederherstellungskosten zu senken, um die Geschäftskontinuität zu optimieren und die Einhaltung gesetzlicher Vorschriften und behördlicher Auflagen zu gewährleisten. Sie können es verwenden AWS Resilience Hub , um Folgendes zu tun:

- Analysieren Sie Ihre Infrastruktur und erhalten Sie Empfehlungen zur Verbesserung der Ausfallsicherheit Ihrer Anwendungen. Neben architektonischen Anleitungen zur Verbesserung der Ausfallsicherheit Ihrer Anwendungen enthalten die Empfehlungen auch Code für die Einhaltung Ihrer Ausfallsicherheitsrichtlinien und die Implementierung von Tests, Alarmen und Standardarbeitsanweisungen (SOPs), die Sie zusammen mit Ihrer Anwendung in Ihrer Integrations- und Bereitstellungspipeline (CI/CD) bereitstellen und ausführen können.
- Evaluieren Sie die Ziele für Recovery Time Objective (RTO) und Recovery Point Objective (RPO) unter verschiedenen Bedingungen.
- Optimieren Sie die Geschäftskontinuität und reduzieren Sie gleichzeitig die Wiederherstellungskosten.
- Identifizieren und lösen Sie Probleme, bevor sie in der Produktion auftreten.

Nachdem Sie eine Anwendung in der Produktion bereitgestellt haben, können Sie sie AWS Resilience Hub zu Ihrer CI/CD-Pipeline hinzufügen, um jeden Build zu validieren, bevor er für die Produktion freigegeben wird.

Wie funktioniert AWS Resilience Hub

Das folgende Diagramm bietet einen allgemeinen Überblick über die AWS Resilience Hub Funktionsweise.


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

Describe

Beschreiben Sie Ihre Anwendung, indem Sie Ressourcen aus AWS CloudFormation Stacks, Terraform-Statusdateien oder Amazon Elastic Kubernetes Service Service-Clustern importieren. Sie können auch aus Anwendungen wählen, die bereits in definiert sind. AWS Resource Groups AWS Service Catalog AppRegistry

Definieren

Definieren Sie die Ausfallsicherheitsrichtlinien für Ihre Anwendungen. Diese Richtlinien beinhalten RTO und RPO zielen auf Störungen in Anwendungen, Infrastruktur, Availability Zone und Regionen ab. Diese Ziele werden verwendet, um abzuschätzen, ob die Anwendung die Stabilitätsrichtlinie erfüllt.

Bewerten

Nachdem Sie Ihre Anwendung beschrieben und ihr eine Resilienzrichtlinie beigefügt haben, führen Sie eine Resilienzbewertung durch. Bei der AWS Resilience Hub Bewertung werden bewährte Verfahren aus dem AWS Well-Architected Framework verwendet, um die Komponenten einer Anwendung zu analysieren und potenzielle Schwächen bei der Widerstandsfähigkeit aufzudecken. Diese Schwächen können durch eine unvollständige Einrichtung der Infrastruktur, durch Fehlkonfigurationen oder durch Situationen verursacht werden, in denen zusätzliche Konfigurationsverbesserungen erforderlich sind. Um die Ausfallsicherheit zu verbessern, aktualisieren Sie Ihre Anwendungs- und Ausfallsicherheitsrichtlinie gemäß den Empfehlungen aus dem Bewertungsbericht. Zu den Empfehlungen gehören Konfigurationen von Komponenten, Alarme, Tests und Wiederherstellung. SOPs Anschließend können Sie eine weitere Bewertung durchführen und die Ergebnisse mit dem vorherigen Bericht vergleichen, um festzustellen, wie stark sich die Ausfallsicherheit verbessert. Wiederholen Sie diesen Vorgang, bis Ihre geschätzte Arbeitslast RTO und Ihre geschätzte Arbeitslast Ihren RPO Zielvorgaben RTO entsprechen. RPO

Bestätigen

Führen Sie Tests durch, um die Widerstandsfähigkeit Ihrer AWS Ressourcen und die Zeit zu messen, die für die Wiederherstellung nach Anwendungen, Infrastruktur, Availability Zone und AWS-Region Vorfällen benötigt wird. Um die Ausfallsicherheit zu messen, simulieren diese Tests Ausfälle Ihrer Ressourcen. AWS Beispiele für Ausfälle sind Netzwerkfehler, Failovers, gestoppte Prozesse, RDS Amazon-Startwiederherstellung und Probleme mit Ihrer Availability Zone.

Ansehen und verfolgen

Nachdem Sie eine AWS Anwendung in der Produktion bereitgestellt haben, können Sie AWS Resilience Hub sie verwenden, um die Ausfallsicherheit der Anwendung weiter zu verfolgen.

Wenn ein Ausfall auftritt, kann der Bediener den Ausfall anzeigen AWS Resilience Hub und den zugehörigen Wiederherstellungsprozess starten.

AWS Resilience Hub — Resilienztests

AWS Resilience Hub ermöglicht es Ihnen, Tests und Experimente mit Amazon Fault Injection Service (AWS FIS) an Ihren AWS Workloads durchzuführen und eine optimale Ausfallsicherheit aufrechtzuerhalten. Diese Tests stress eine Anwendung, indem sie störende Ereignisse auslösen, sodass Sie beobachten können, wie Ihre Anwendung reagiert. AWS FIS bietet mehrere vorgefertigte Szenarien und eine große Auswahl an Aktionen, die zu Störungen führen. Darüber hinaus enthält es auch Steuerungen und Leitplanken, die Sie für die Durchführung der Experimente in der Produktion benötigen. Die Steuerungen und Leitplanken beinhalten Optionen, mit denen Sie ein automatisches Rollback durchführen oder das Experiment beenden können, wenn bestimmte Bedingungen erfüllt sind. Um mit dem Ausführen von Experimenten von der AWS Resilience Hub Konsole aus AWS FIS zu beginnen, müssen Sie die im the section called “Voraussetzungen” Abschnitt definierten Voraussetzungen erfüllen.

In der folgenden Tabelle sind alle verfügbaren AWS FIS Optionen im Navigationsbereich sowie die Links zur zugehörigen AWS FIS Dokumentation aufgeführt, die die Verfahren für den Einstieg in die Verwendung von AWS FIS Tests über die AWS Resilience Hub Konsole enthält.

AWS FIS Optionen und Verweise im Navigationsmenü

AWS FIS Option für das Navigationsmenü	AWS FIS Dokumentation
Resilienztests	Erstellen Sie eine Versuchsvorlage
Szenario-Bibliothek	AWS FIS Bibliothek
Vorlagen für Experimente	Experimentiervorlagen für AWS FIS

In der folgenden Tabelle sind alle verfügbaren AWS FIS Optionen aus dem Dropdownmenü im Abschnitt Resilienztests sowie die Links zur zugehörigen AWS FIS Dokumentation aufgeführt, die die Verfahren für den Einstieg in die Verwendung von AWS FIS Tests über die AWS Resilience Hub Konsole enthält.

AWS FIS Optionen und Referenzen im Dropdownmenü

AWS FIS Option im Dropdownmenü	AWS FIS Dokumentation
Experimentvorlage erstellen	Erstellen Sie eine Experimentvorlage
Erstellen Sie ein Experiment anhand eines Szenarios	Verwenden eines Szenarios

AWS Resilience Hub Konzepte

Diese Konzepte können Ihnen helfen, den Ansatz AWS Resilience Hub von zu verstehen, mit dem Sie die Ausfallsicherheit von Anwendungen verbessern und Anwendungsausfälle verhindern können.

Ausfallsicherheit

Die Fähigkeit, die Verfügbarkeit aufrechtzuerhalten und die Wiederherstellung nach Software- und Betriebsunterbrechungen innerhalb eines festgelegten Zeitrahmens zu gewährleisten.

Ziel des Wiederherstellungspunkts (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Ziel der Wiederherstellungszeit (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes. Dies bestimmt, welches Zeitfenster als akzeptables Zeitfenster angesehen wird, wenn der Dienst nicht verfügbar ist.

Voraussichtliches Ziel für die Wiederherstellung des Workloads

Das geschätzte Ziel für die Workload-Wiederherstellungszeit (geschätzte ArbeitslastRTO) ist RTO das Ziel, das Ihre Anwendung auf der Grundlage der importierten Anwendungsdefinition voraussichtlich erreichen wird. Führen Sie anschließend eine Bewertung durch.

Voraussichtlicher Zielwert für die Wiederherstellung der Arbeitslast

Das geschätzte Ziel des Workload-Wiederherstellungspunkts (geschätzte ArbeitslastRPO) ist RPO das Ziel, das Ihre Anwendung auf der Grundlage der importierten Anwendungsdefinition voraussichtlich erreichen wird. Anschließend wird eine Bewertung durchgeführt.

Anwendung

Eine AWS Resilience Hub Anwendung ist eine Sammlung AWS unterstützter Ressourcen, die kontinuierlich überwacht und bewertet werden, um ihre Ausfallsicherheit zu gewährleisten.

Komponente der Anwendung

Eine Gruppe verwandter AWS Ressourcen, die als eine Einheit funktionieren und ausfallen. Wenn Sie beispielsweise über eine Primär- und eine Replikatdatenbank verfügen, gehören beide Datenbanken zu derselben Anwendungskomponente (AppComponent).

AWS Resilience Hub bestimmt, welche AWS Ressourcen zu welchem Typ gehören können. AppComponent Zum Beispiel `DBInstance` kann a gehören, `AWS::ResilienceHub::DatabaseAppComponent` aber nicht zu`AWS::ResilienceHub::ComputeAppComponent`.

Konformitätsstatus der Anwendung

AWS Resilience Hub meldet die folgenden Konformitätsstatustypen für Ihre Anwendungen.

Richtlinie erfüllt

Es wird davon ausgegangen, dass der Antrag die in der Richtlinie festgelegten RPO Ziele erfüllt. RTO Alle seine Bestandteile entsprechen den definierten politischen Zielen. Sie haben beispielsweise ein RTO RPO Ziel von 24 Stunden für Störungen in allen AWS Regionen ausgewählt. AWS Resilience Hub kann sehen, dass Ihre Backups in Ihre Fallback-Region kopiert wurden. Es wird weiterhin von Ihnen erwartet, dass Sie die Wiederherstellung nach einem Backup nach der Standardprozedur (SOP) durchführen und diese auch testen und zeitlich festlegen. Dies ist in den Betriebsempfehlungen enthalten und Teil Ihres allgemeinen Resilienz-Scores.

Richtlinie verletzt

Es konnte nicht davon ausgegangen werden, dass der Antrag die RTO in der Richtlinie festgelegten RPO Ziele erfüllt. Einer oder mehrere davon entsprechen AppComponents nicht den politischen

Zielen. Sie haben beispielsweise ein RTO RPO Ziel von 24 Stunden für Unterbrechungen in allen AWS Regionen ausgewählt, aber Ihre Datenbankkonfiguration beinhaltet keine regionsübergreifende Wiederherstellungsmethode, wie z. B. eine globale Replikation und Backup-Kopien.

Nicht bewertet

Der Antrag erfordert eine Bewertung. Es wird derzeit nicht bewertet oder verfolgt.

Es wurden Änderungen festgestellt

Es gibt eine neue veröffentlichte Version der Anwendung, die noch nicht bewertet wurde.

Erkennung von Abweichungen

AWS Resilience Hub führt während der Durchführung einer Bewertung Ihrer Anwendung eine Drift-Benachrichtigung durch, um zu überprüfen, ob sich die Änderungen an den AppComponent Konfigurationen auf den Konformitätsstatus Ihrer Anwendung ausgewirkt haben. Darüber hinaus werden Änderungen wie das Hinzufügen oder Löschen von Ressourcen in den Eingabequellen der Anwendung überprüft und erkannt und darüber informiert. Zum Vergleich AWS Resilience Hub wird die vorherige Bewertung verwendet, bei der die Anwendungskomponente die Richtlinie erfüllte. AWS Resilience Hub erkennt die folgenden Arten von Abweichungen:

- Abweichung von der Anwendungsrichtlinie — Bei dieser Abweichung werden alle Personen identifiziert AppComponents , die die Richtlinie in der vorherigen Bewertung erfüllten, in der aktuellen Bewertung jedoch nicht eingehalten haben.
- Drift bei Anwendungsressourcen — Dieser Drift-Typ identifiziert alle Drift-Ressourcen in der aktuellen Anwendungsversion.

Bewertung der Resilienz

AWS Resilience Hub verwendet eine Liste von Lücken und möglichen Abhilfemaßnahmen, um die Wirksamkeit einer ausgewählten Strategie zur Wiederherstellung und Fortführung nach einer Katastrophe zu messen. Dabei wird der Konformitätsstatus der einzelnen Anwendungskomponenten oder Anwendungen anhand der Richtlinie bewertet. Dieser Bericht enthält Empfehlungen zur Kostenoptimierung und Hinweise auf mögliche Probleme.

Bewertung der Resilienz

AWS Resilience Hub generiert eine Bewertung, die angibt, wie genau Ihre Anwendung unseren Empfehlungen zur Einhaltung der Stabilitätsrichtlinien, Alarme, Standardarbeitsanweisungen (SOPs) und Tests für die Anwendung entspricht.

Art der Störung

AWS Resilience Hub hilft Ihnen bei der Bewertung der Widerstandsfähigkeit gegen die folgenden Arten von Ausfällen:

Anwendung

Die Infrastruktur ist intakt, aber die Anwendung oder der Software-Stack funktioniert nicht wie gewünscht. Dies kann nach der Bereitstellung von neuem Code, Konfigurationsänderungen, Datenbeschädigung oder Fehlfunktionen nachgelagerter Abhängigkeiten auftreten.

Cloud-Infrastruktur

Die Cloud-Infrastruktur funktioniert aufgrund eines Ausfalls nicht wie erwartet. Ein Ausfall kann aufgrund eines lokalen Fehlers in einer oder mehreren Komponenten auftreten. In den meisten Fällen wird diese Art von Ausfall durch einen Neustart, Recycling oder erneutes Laden der fehlerhaften Komponenten behoben.

Unterbrechung der Cloud-Infrastruktur

Eine oder mehrere Availability Zones sind nicht verfügbar. Diese Art von Ausfall kann behoben werden, indem zu einer anderen Availability Zone gewechselt wird.

Vorfall in der Cloud-Infrastrukturregion

Eine oder mehrere Regionen sind nicht verfügbar. Diese Art von Vorfall kann behoben werden, indem Sie zu einer anderen wechseln AWS-Region.

Experimente zur Fehlerinjektion

AWS Resilience Hub empfiehlt Tests zur Überprüfung der Widerstandsfähigkeit von Anwendungen gegenüber verschiedenen Arten von Ausfällen. Zu diesen Ausfällen gehören Anwendungen, Infrastruktur, Availability Zones (AZ) oder AWS-Region Vorfälle von Anwendungskomponenten.

Mit diesen Experimenten können Sie Folgendes tun:

- Injizieren Sie einen Fehler.
- Stellen Sie sicher, dass Alarme einen Ausfall erkennen können.
- Stellen Sie sicher, dass die Wiederherstellungsverfahren oder Standardarbeitsanweisungen (SOPs) ordnungsgemäß funktionieren, um die Anwendung nach dem Ausfall wiederherzustellen.

Tests zur SOPs Messung der geschätzten Arbeitslast RTO und der geschätzten ArbeitslastRPO. Sie können verschiedene Anwendungskonfigurationen testen und messen, ob die Ergebnisse RTO den in Ihrer Richtlinie definierten Zielen entsprechen. RPO

SOP

Bei einer SOP Standardarbeitsanweisung () handelt es sich um eine Reihe von Schritten, mit denen Sie Ihre Anwendung bei einem Ausfall oder einem Alarm effizient wiederherstellen können. Auf der Grundlage der Anwendungsbeurteilung AWS Resilience Hub empfiehlt es eine Reihe von Maßnahmen, SOPs und es wird empfohlen, diese SOPs im Vorfeld einer Unterbrechung vorzubereiten, zu testen und zu messen, um eine zeitnahe Wiederherstellung zu gewährleisten.

AWS Resilience Hub Personas

Die Entwicklung einer Unternehmensanwendung erfordert die Zusammenarbeit verschiedener funktionsübergreifender Teams wie Infrastruktur, Geschäftskontinuität, Anwendungsverantwortlicher und anderer Beteiligter, die für die Überwachung der Anwendungen verantwortlich sind. Die verschiedenen Personen aus den verschiedenen Teams tragen zur Entwicklung und Verwaltung von Anwendungen bei AWS Resilience Hub und haben jeweils unterschiedliche Rollen und Verantwortlichkeiten. Weitere Informationen zur Vergabe von Berechtigungen an verschiedene Personas finden Sie unter. the section called “AWS Resilience Hub Referenz zu Personas und IAM Berechtigungen”

Für den Einstieg in die Erstellung von Anwendungen und die Durchführung von Assessments empfehlen wir Ihnen AWS Resilience Hub, die folgenden Personas zu erstellen:

- Infrastrukturanwendungsmanager — Benutzer mit dieser Persona sind für die Einrichtung, Konfiguration und Wartung der Infrastruktur- und Anwendungsressourcen verantwortlich und gewährleisten so die Zuverlässigkeit und Sicherheit der Anwendung. Zu ihren Aufgaben gehören unter anderem:
  - Sicherstellung, dass die Anwendungen regelmäßig bereitgestellt und aktualisiert werden

    - Überwachung der Systemleistung
    - Beheben von -Problemen
    - Implementierung von Sicherungs- und Notfallwiederherstellungsplänen
- Business Continuity Manager — Benutzer mit dieser Persona sind dafür verantwortlich, Anwendungsrichtlinien zu diktieren und die geschäftliche Wichtigkeit von Anwendungen zu bestimmen. Zu ihren Aufgaben gehören unter anderem:
    - Treffen wichtiger Entscheidungen bei der Festlegung von Richtlinien
    - Bewertung der Geschäftspritikalität
    - Zuweisung von Ressourcen für kritische Anwendungen
    - Bewertung und Verwaltung von Risiken
- Anwendungseigentümer — Benutzer mit dieser Persona sind dafür verantwortlich, dass ihre Anwendungen hochverfügbar und zuverlässig sind. Zu ihren Aufgaben gehören unter anderem:
    - Definition wichtiger Leistungskennzahlen zur Messung und Überwachung der Anwendungsleistung und zur Identifizierung von Engpässen
    - Organisation von Schulungen für mehrere Interessengruppen
    - Stellen Sie sicher, dass die folgende Dokumentation up-to-date:
        - Anwendungsarchitektur
        - Bereitstellungsprozesse
        - Konfigurationen überwachen
        - Techniken zur Leistungsoptimierung
- Nur-Lese-Zugriff — Benutzer mit dieser Persona haben nur Leseberechtigungen. Zu ihren Aufgaben gehört es, die Leistung und den Zustand einer Anwendung transparent und im Blick zu behalten, indem sie den Resilienzwert sowie betriebliche Empfehlungen und Empfehlungen zur Ausfallsicherheit überwachen. Darüber hinaus sind sie auch dafür verantwortlich, Probleme, Trends und Verbesserungsmöglichkeiten zu identifizieren, um sicherzustellen, dass die Anwendung den Unternehmenszielen entspricht.

AWS Resilience Hub unterstützte Ressourcen

Ressourcen, die sich im Fall einer Unterbrechung auf die Anwendungsleistung auswirken, werden vollständig durch Ressourcen der AWS Resilience Hub obersten Ebene wie `AWS::RDS::DBInstance` und `AWS::RDS::DBCluster` unterstützt.

Weitere Informationen zu den Berechtigungen, die erforderlich sind AWS Resilience Hub , um Ressourcen aus allen unterstützten Diensten in Ihre Bewertung einzubeziehen, finden Sie unterthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

AWS Resilience Hub unterstützt Ressourcen aus den folgenden AWS Diensten:

- Datenverarbeitung
  - Amazon Elastic Compute Cloud (AmazonEC2)

    > **Note**
    >
    > AWS Resilience Hub unterstützt das alte Format Amazon Resource Name (ARN) für den Zugriff auf EC2 Amazon-Ressourcen nicht. Das neue ARN Format verwendet Ihre AWS Konto-ID und ermöglicht die erweiterte Möglichkeit, Ressourcen in Ihrem Cluster zu taggen. Außerdem werden die Kosten für Dienste und Aufgaben erfasst, die in Ihrem Cluster ausgeführt werden.
    >
    > - Altes Format (veraltet) — `arn:aws:ec2:<region>::instance/<instance-id>`
    > - Neues Format — `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`
    >
    > Weitere Informationen zum neuen ARN Format finden Sie unter Migration Ihrer ECS Amazon-Bereitstellung auf das neue Format ARN und unter Resource ID.

  - AWS Lambda
  - Amazon Elastic Kubernetes Service (Amazon) EKS
  - Amazon Elastic Container Service (AmazonECS)
  - AWS Step Functions
- Datenbank
  - Amazon Relational Database Service (AmazonRDS)
  - Amazon-DynamoDB
  - Amazon DocumentDB
- Netzwerk und Bereitstellung von Inhalten
  - Amazon Route 53
  - Elastic Load Balancing
  - Übersetzung von Netzwerkadressen () NAT
- Speicher

  - Amazon Elastic Block Store (AmazonEBS)
  - Amazon Elastic File System (AmazonEFS)
  - Amazon-Simple-Storage-Service (Amazon-S3)
  - Amazon FSx für Windows-Dateiserver
- Weitere
  - APIAmazon-Gateway
  - Amazon Route 53-Controller für die Anwendungswiederherstellung (Amazon Route 53ARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS Elastische Notfallwiederherstellung

> **Note**
>
> - AWS Resilience Hub bietet zusätzliche Transparenz für Ihre Anwendungsressourcen, indem Sie die unterstützten Instanzen der einzelnen Ressourcen einsehen können. Darüber hinaus AWS Resilience Hub bietet es genauere Empfehlungen zur Ausfallsicherheit, indem es eine eindeutige Instanz jeder Ressource identifiziert und gleichzeitig die Ressourceninstanzen während des Bewertungsprozesses ermittelt. Weitere Informationen zum Hinzufügen von Ressourceninstanzen zu Ihrer Anwendung finden Sie unterAWS Resilience Hub Anwendungsressourcen bearbeiten.
> - AWS Resilience Hub unterstützt Amazon EKS und Amazon ECS on AWS Fargate.
> - AWS Resilience Hub unterstützt die Bewertung von AWS Backup Ressourcen im Rahmen der folgenden Dienste:
>   - Amazon EBS
>   - Amazon EFS
>   - Amazon S3
>   - Globale Amazon Aurora Aurora-Datenbank
>   - Amazon-DynamoDB
>   - RDSAmazon-Dienste
>   - Amazon FSx für Windows-Dateiserver

- Amazon Route 53 ARC in AWS Resilience Hub bewertet nur Amazon DynamoDB Global, Elastic Load BalancingRDS, Amazon und Gruppen. AWS Auto Scaling
- AWS Resilience Hub Um die regionsübergreifenden Ressourcen zu bewerten, gruppieren Sie die Ressourcen in einer einzigen Anwendungskomponente. Weitere Informationen zu den Ressourcen, die von den einzelnen AWS Resilience Hub Anwendungskomponenten unterstützt werden, und zur Gruppierung von Ressourcen finden Sie unter. Gruppieren von Ressourcen in einer Anwendungskomponente
- Unterstützt derzeit AWS Resilience Hub keine regionsübergreifenden Bewertungen für EKS Amazon-Cluster, wenn sich entweder der EKS Amazon-Cluster befindet oder wenn die Anwendung in einer Region erstellt wurde, für die Opt-In aktiviert AWS ist.
- Derzeit werden nur die folgenden Kubernetes-Ressourcentypen AWS Resilience Hub bewertet:
  - Bereitstellungen
  - ReplicaSets
  - Pods

AWS Resilience Hub ignoriert die folgenden Ressourcentypen:

- Ressourcen, die sich nicht auf die geschätzte Arbeitslast RTO oder die geschätzte Arbeitslast auswirken RPO — Ressourcen wie`AWS::RDS::DBParameterGroup`, die sich nicht auf die geschätzte Arbeitslast RTO oder die geschätzte Arbeitslast auswirkenRPO, werden von AWS Resilience Hub ignoriert.
- Ressourcen der obersten Ebene — importiert AWS Resilience Hub nur Ressourcen der obersten Ebene, da sie andere Eigenschaften ableiten können, indem sie die Eigenschaften von Ressourcen der obersten Ebene abfragen. Zum Beispiel `AWS::ApiGateway::RestApi` und `AWS::ApiGatewayV2::Api` sind unterstützte Ressourcen für Amazon API Gateway. Es `AWS::ApiGatewayV2::Stage` handelt sich jedoch nicht um eine Ressource der obersten Ebene. Daher wird sie nicht von AWS Resilience Hub importiert.

> **Note**
>
> Nicht unterstützte Ressourcen

- Sie können nicht mehrere Ressourcen mithilfe von Ressourcen AWS Resource Groups (Amazon Route 53 RecordSets und API -GWHTTP) und Amazon Aurora Global identifizieren. Wenn Sie diese Ressourcen im Rahmen Ihrer Bewertung analysieren möchten, müssen Sie die Ressource manuell zur Anwendung hinzufügen. Wenn Sie jedoch Amazon Aurora Global-Ressourcen zur Bewertung hinzufügen, müssen diese mit der Anwendungskomponente der RDS Amazon-Instance gruppiert werden. Weitere Informationen zur Bearbeitung von Ressourcen finden Sie unterthe section called “Anwendungsressourcen bearbeiten”.
- Diese Ressourcen können sich auf die Anwendungswiederherstellung auswirken, werden aber AWS Resilience Hub derzeit nicht vollständig von unterstützt. AWS Resilience Hub bemüht sich, Benutzer vor nicht unterstützten Ressourcen zu warnen, wenn die Anwendung von einem AWS CloudFormation Stack, einer Terraform-Statusdatei oder einer Anwendung unterstützt wird. AWS Resource Groups AppRegistry

Erste Schritte

In diesem Abschnitt wird beschrieben, wie Sie mit der Verwendung beginnen AWS Resilience Hub. Dazu gehört das Erstellen von AWS Identity and Access Management (IAM-) Berechtigungen für ein Konto.

Themen

Voraussetzungen

Bevor Sie das verwenden können AWS Resilience Hub, müssen Sie die folgenden Voraussetzungen erfüllen:

- AWS Konten — Erstellen Sie ein oder mehrere AWS Konten für jeden Kontotyp (primäres, sekundäres Konto, Ressourcenkonto), das Sie verwenden möchten. AWS Resilience Hub Weitere Informationen zum Erstellen und Verwalten von AWS Konten finden Sie im Folgenden:
  - AWS Erstbenutzer — Erste Schritte: Sind Sie ein AWS Erstbenutzer?
  - AWS Konto verwalten — https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management (IAM-) Berechtigungen — Nachdem Sie die AWS Konten erstellt haben, müssen Sie die erforderlichen Rollen und IAM-Berechtigungen für jedes der von Ihnen erstellten Konten konfigurieren. Wenn Sie beispielsweise ein AWS Konto für den Zugriff auf Anwendungsressourcen erstellt haben, müssen Sie eine neue Rolle einrichten und die erforderlichen IAM-Berechtigungen für den AWS Resilience Hub Zugriff auf die Anwendungsressourcen von Ihrem Konto aus konfigurieren. Weitere Informationen zu IAM-Berechtigungen finden Sie unterthe section called “Wie funktioniert AWS Resilience Hub mit IAM”. Weitere Informationen zum Hinzufügen einer Richtlinie zur Rolle finden Sie unter. the section called “Definition einer Vertrauensrichtlinie mithilfe einer JSON Datei”

  Um schnell mit dem Hinzufügen von IAM-Berechtigungen zu Benutzern, Gruppen und Rollen zu beginnen, können Sie unsere AWS verwalteten Richtlinien () the section called “AWS verwaltete Richtlinien” verwenden. Es ist einfacher, AWS verwaltete Richtlinien zu verwenden, um allgemeine Anwendungsfälle abzudecken, die in Ihrem Fall verfügbar sind, AWS-Konto als Richtlinien selbst zu

schreiben. AWS Resilience Hub fügt einer AWS verwalteten Richtlinie zusätzliche Berechtigungen hinzu, um die Unterstützung auf andere AWS Dienste auszudehnen und neue Funktionen hinzuzufügen. Daher gilt:

- Wenn Sie bereits Kunde sind und möchten, dass Ihre Anwendung die neuesten Verbesserungen im Rahmen Ihrer Bewertung nutzt, müssen Sie eine neue Version der Anwendung veröffentlichen und anschließend eine neue Bewertung durchführen. Weitere Informationen finden Sie unter den folgenden Themen:
  - the section called “Veröffentlichen Sie eine neue Anwendungsversion”
  - the section called “Durchführung von Resilienzbewertungen”
- Wenn Sie keine AWS verwalteten Richtlinien verwenden, um Benutzern, Gruppen und Rollen die entsprechenden IAM-Berechtigungen zuzuweisen, müssen Sie diese Berechtigungen manuell konfigurieren. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unterthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Fügen Sie eine Anwendung hinzu zu AWS Resilience Hub

AWS Resilience Hub bietet eine Bewertung und Validierung der Ausfallsicherheit, die sich in Ihren Softwareentwicklungszyklus integrieren lässt. AWS Resilience Hub hilft Ihnen dabei, Ihre AWS Anwendungen proaktiv vorzubereiten und vor Störungen zu schützen, und zwar durch:

- Aufdeckung von Schwächen im Bereich Resilienz
- Schätzung, ob Ihr angestrebtes Ziel für die Wiederherstellungszeit (RTO) und das Ziel für den Wiederherstellungspunkt (RPO) erreicht werden können.
- Lösung von Problemen, bevor sie in die Produktion aufgenommen werden.

In diesem Abschnitt erfahren Sie, wie Sie eine Anwendung hinzufügen. Sie sammeln Ressourcen aus einer vorhandenen Anwendung, AWS CloudFormation Stacks oder einer vorhandenen Anwendung AppRegistry und erstellen eine entsprechende Ausfallsicherheitsrichtlinie. AWS Resource Groups Nachdem Sie eine Anwendung beschrieben haben, können Sie sie veröffentlichen und einen Bewertungsbericht über die Ausfallsicherheit Ihrer Anwendung erstellen. AWS Resilience Hub Anschließend können Sie die Empfehlungen aus der Bewertung verwenden, um die Ausfallsicherheit zu verbessern. Sie können eine weitere Bewertung durchführen, die Ergebnisse vergleichen und dann so lange iterieren, bis die geschätzte Arbeitslast RTO und die geschätzte Arbeitslast Ihren RPO Zielvorgaben entsprechenRTO. RPO

Themen

Schritt 1: Fügen Sie zunächst eine Anwendung hinzu

Beschreiben Sie zunächst die Details Ihrer AWS Anwendung und führen Sie einen Bericht zur Bewertung der Resilienz aus. AWS Resilience Hub

Wählen Sie zunächst auf der AWS Resilience Hub Startseite unter Erste Schritte die Option Anwendung hinzufügen aus.

Weitere Informationen zu den damit verbundenen Kosten und der Abrechnung finden Sie unter AWS Resilience Hub Preise. AWS Resilience Hub

Beschreiben Sie die Einzelheiten Ihrer Bewerbung in AWS Resilience Hub

In diesem Abschnitt erfahren Sie, wie Sie die Details Ihrer bestehenden AWS Anwendung in beschreiben AWS Resilience Hub.

Um die Details Ihrer Bewerbung zu beschreiben

1. Geben Sie einen Namen für die Anwendung ein.
2. (Optional) Geben Sie eine Beschreibung für die Anwendung ein.

Next

Schritt 2: Wie wird Ihre Anwendung verwaltet?

Schritt 2: Wie wird Ihre Anwendung verwaltet?

Zusätzlich zu AWS CloudFormation Stacks AWS Resource Groups, AppRegistry Anwendungen und Terraform-Statusdateien können Sie Ressourcen hinzufügen, die sich auf Amazon Elastic Kubernetes Service (Amazon) -Clustern befinden. EKS Das heißt, AWS Resilience Hub ermöglicht es Ihnen, Ressourcen, die sich auf Ihren EKS Amazon-Clustern befinden, als optionale Ressourcen hinzuzufügen. Dieser Abschnitt enthält die folgenden Optionen, mit denen Sie den Standort Ihrer Anwendungsressourcen ermitteln können.

- Ressourcensammlungen — Wählen Sie diese Option, wenn Sie Ressourcen aus einer der Ressourcensammlungen suchen möchten. Zu den Ressourcensammlungen gehören AWS CloudFormation Stapel AWS Resource Groups, AppRegistry Anwendungen und Terraform-Statusdateien.

  Wenn Sie diese Option auswählen, müssen Sie eines der Verfahren unter ausführen. the section called “Fügen Sie Ressourcensammlungen hinzu”
- EKSnur — Wählen Sie diese Option, wenn Sie Ressourcen aus Namespaces innerhalb der Amazon-Cluster ermitteln möchten. EKS

  Wenn Sie diese Option wählen, müssen Sie das Verfahren in abschließen the section called “Fügen Sie Cluster hinzu EKS”
- Ressourcensammlungen & EKS — Wählen Sie diese Option, wenn Sie Ressourcen aus einer der Ressourcensammlungen und EKS Amazon-Clustern entdecken möchten.

  Wenn Sie diese Option auswählen, führen Sie eines der Verfahren unter the section called “Fügen Sie Ressourcensammlungen hinzu” und schließen Sie dann das Verfahren unter abthe section called “Fügen Sie Cluster hinzu EKS”.

> **Note**
>
> Informationen zur Anzahl der pro Anwendung unterstützten Ressourcen finden Sie unter Service Quotas.

Next

Schritt 3: Fügen Sie Ihrer AWS Resilience Hub Anwendung Ressourcen hinzu

Schritt 3: Fügen Sie Ihrer AWS Resilience Hub Anwendung Ressourcen hinzu

In diesem Abschnitt werden die folgenden Optionen beschrieben, die Sie als Grundlage für Ihre Anwendungsstruktur verwenden können:

- the section called “Fügen Sie Ressourcensammlungen hinzu”
- the section called “Fügen Sie Cluster hinzu EKS”

Fügen Sie Ressourcensammlungen hinzu

In diesem Abschnitt werden die folgenden Methoden beschrieben, mit denen Sie die Grundlage für Ihre Anwendungsstruktur bilden:

- Verwendung von AWS CloudFormation Stacks
- Verwenden AWS Resource Groups
- AppRegistry Anwendungen verwenden
- Terraform-Statusdateien verwenden
- Verwenden einer vorhandenen Anwendung AWS Resilience Hub

Verwendung von AWS CloudFormation Stacks

Wählen Sie die AWS CloudFormation Stacks aus, die die Ressourcen enthalten, die Sie in der von Ihnen beschriebenen Anwendung verwenden möchten. Die Stapel können aus dem stammen AWS-Konto , den Sie zur Beschreibung der Anwendung verwenden, oder sie können aus verschiedenen Konten oder verschiedenen Regionen stammen.

Um die Ressourcen zu ermitteln, die die Grundlage Ihrer Anwendungsstruktur bilden

1. Wählen Sie CloudFormation Stacks aus, um Ihre stackbasierten Ressourcen zu ermitteln.
2. Wählen Sie Stacks aus der Drop-down-Liste Stacks auswählen aus, die mit Ihrer Region verknüpft sind. AWS-Konto

   Um Stacks zu verwenden, die sich in einer anderen AWS-Konto, einer anderen Region oder in beiden befinden, geben Sie den Amazon-Ressourcennamen (ARN) des Stacks in das Feld Stapel außerhalb der AWS Region hinzufügen ein und wählen Sie dann Stapel ARN hinzufügen.

Weitere Informationen zu ARNs finden Sie unter Amazon Resource Names (ARNs) in der AWS Allgemeinen Referenz.

Verwenden AWS Resource Groups

Wählen Sie AWS Resource Groups die aus, die die Ressourcen enthalten, die Sie in der von Ihnen beschriebenen Anwendung verwenden möchten.

Um die Ressourcen zu ermitteln, die die Grundlage Ihrer Anwendungsstruktur bilden

1. Wählen Sie Ressourcengruppen aus, um herauszufinden AWS Resource Groups , welche die Ressourcen enthalten.
2. Wählen Sie Ressourcen aus der Dropdownliste Ressourcengruppen auswählen aus.

   Um diese zu verwenden, AWS Resource Groups die sich in einer anderen AWS-Konto, anderen Region oder in beiden befinden, geben Sie den Amazon-Ressourcennamen (ARN) des Stacks in das ARN Feld Ressourcengruppe ein und wählen Sie dann Ressourcengruppe hinzufügen ARN. Weitere Informationen zu ARNs finden Sie unter Amazon Resource Names (ARNs) in der AWS Allgemeinen Referenz.

AppRegistry Anwendungen verwenden

Sie können jeweils nur eine AppRegistry Anwendung hinzufügen.

Wählen Sie die AppRegistry Anwendungen aus, die die Ressourcen enthalten, die Sie in der von Ihnen beschriebenen Anwendung verwenden möchten.

Um die Ressourcen zu ermitteln, die die Grundlage Ihrer Anwendungsstruktur bilden

1. Wählen Sie AppRegistrydiese Option, um aus einer Liste von Anwendungen auszuwählen, die in erstellt wurden AppRegistry.
2. Wählen Sie in der Dropdownliste Anwendung auswählen die Anwendungen aus AppRegistry, die in erstellt wurden. Sie können jeweils nur eine Anwendung auswählen.

Terraform-Statusdateien verwenden

Wählen Sie die Terraform-Statusdatei aus, die Ihre S3-Bucket-Ressourcen enthält, die Sie in der von Ihnen beschriebenen Anwendung verwenden möchten. Sie können zum Speicherort Ihrer Terraform-

Statusdatei navigieren oder einen Link zu einer Terraform-Statusdatei bereitstellen, auf die Sie Zugriff haben und die sich in einer anderen Region befindet.

> **Note**
>
> AWS Resilience Hub unterstützt die Terraform-Statusdateiversion und höher. `0.12`

Um die Ressourcen zu entdecken, die die Grundlage Ihrer Anwendungsstruktur bilden

1. Wählen Sie Terraform-Statusdateien aus, um Ihre S3-Bucket-Ressourcen zu ermitteln.
2. Wählen Sie im Abschnitt Statusdateien auswählen die Option S3 durchsuchen, um zum Speicherort Ihrer Terraform-Statusdatei zu navigieren.

   Um Terraform-Statusdateien zu verwenden, die sich in einer anderen Region befinden, geben Sie den Link zum Speicherort der Terraform-Statusdatei im URLS3-Feld an und wählen Sie S3 hinzufügen. URL

   Das Limit für Terraform-Statusdateien liegt bei 4 Megabyte (MB).
3. Wählen Sie Ihren S3-Bucket im Bereich Buckets aus.
4. Wählen Sie im Bereich Objekte einen Schlüssel aus und wählen Sie Wählen aus.

Verwenden Sie eine bestehende AWS Resilience Hub Anwendung

Verwenden Sie zunächst eine vorhandene Anwendung.

Um die Ressourcen zu entdecken, die die Grundlage Ihrer Anwendungsstruktur bilden

1. Wählen Sie Bestehende Anwendung aus, um Ihre Anwendung aus einer vorhandenen Anwendung zu erstellen.
2. Wählen Sie eine Anwendung aus der Dropdownliste Bestehende Anwendung auswählen aus.

Fügen Sie Cluster hinzu EKS

In diesem Abschnitt wird die Verwendung von EKS Amazon-Clustern als Grundlage für Ihre Anwendungsstruktur beschrieben.

> **Note**
>
> Sie benötigen EKS Amazon-Berechtigungen und zusätzliche IAM Rollen, um eine Verbindung zum EKS Amazon-Cluster herzustellen. Weitere Informationen zum Hinzufügen von EKS Amazon-Berechtigungen für einzelne Konten und kontoübergreifende Berechtigungen sowie zu zusätzlichen IAM Rollen für die Verbindung mit dem Cluster finden Sie in den folgenden Themen:
>
> - AWS Resilience Hub Referenz zu Zugriffsberechtigungen
> - the section called “ AWS Resilience Hub Zugriff auf Ihren EKS Amazon-Cluster aktivieren”

Wählen Sie die EKS Amazon-Cluster und -Namespaces aus, die die Ressourcen enthalten, die Sie in der von Ihnen beschriebenen Anwendung verwenden möchten. Die EKS Amazon-Cluster können aus dem stammen AWS-Konto , den Sie zur Beschreibung der Anwendung verwenden, oder sie können aus verschiedenen Konten oder verschiedenen Regionen stammen.

> **Note**
>
> AWS Resilience Hub Um Ihre EKS Amazon-Cluster zu bewerten, müssen Sie die entsprechenden Namespaces manuell zu jedem der EKS Amazon-Cluster im Abschnitt EKSCluster und Namespaces hinzufügen. Der Namespace-Name muss exakt mit dem Namespace-Namen auf Ihren EKS Amazon-Clustern übereinstimmen.

So fügen Sie EKS Amazon-Cluster hinzu

1. Wählen Sie in der Dropdownliste EKSCluster auswählen die EKS Amazon-Cluster aus, die mit Ihrer AWS-Konto Region verknüpft sind.
2. Um EKS Amazon-Cluster zu verwenden, die sich in einer anderen AWS-Konto, einer anderen Region oder in beiden befinden, geben Sie den Amazon-Ressourcennamen (ARN) des Stacks in das Feld Kontoübergreifend oder Region ein und wählen Sie dann Hinzufügen EKS ARN. Weitere Informationen zu ARNs finden Sie unter Amazon Resource Names (ARNs) in der AWS Allgemeinen Referenz.

   Weitere Informationen zum Hinzufügen von Berechtigungen für den Zugriff auf regionsübergreifende Amazon Elastic Kubernetes Service Service-Cluster finden Sie unter. the section called “ AWS Resilience Hub Zugriff auf Ihren EKS Amazon-Cluster aktivieren”

Um Namespaces aus den ausgewählten Amazon-Clustern hinzuzufügen EKS

1. Wählen Sie im Abschnitt Namespaces hinzufügen in der Tabelle EKSCluster und Namespaces das Optionsfeld links neben dem EKS Amazon-Clusternamen aus und wählen Sie dann Namespaces aktualisieren.

   Sie können EKS Amazon-Cluster wie folgt identifizieren:

   - EKSClustername — Gibt den Namen der ausgewählten EKS Amazon-Cluster an.
   - Anzahl der Namespaces — Gibt die Anzahl der Namespaces an, die in den Amazon-Clustern ausgewählt wurden. EKS
   - Status — Gibt an, ob AWS Resilience Hub die Namespaces der ausgewählten EKS Amazon-Cluster in Ihre Anwendung aufgenommen wurden. Sie können den Status mithilfe der folgenden Optionen ermitteln:
     - Namespace erforderlich — Zeigt an, dass Sie keine Namespaces aus dem Amazon-Cluster aufgenommen haben. EKS
     - Namespaces hinzugefügt — Zeigt an, dass Sie einen oder mehrere Namespaces aus dem Amazon-Cluster hinzugefügt haben. EKS
2. Um einen Namespace hinzuzufügen, wählen Sie im Dialogfeld Namespaces aktualisieren die Option Neuen Namespace hinzufügen.

   Im Dialogfeld „Namespaces aktualisieren“ werden alle Namespaces, die Sie aus Ihrem EKS Amazon-Cluster ausgewählt haben, als bearbeitbare Option angezeigt.
3. Im Dialogfeld „Namespaces aktualisieren“ haben Sie die folgenden Bearbeitungsoptionen:

   - Um einen neuen Namespace hinzuzufügen, wählen Sie Neuen Namespace hinzufügen und geben Sie dann den Namespace-Namen in das Feld Namespace ein.

     Der Namespace-Name muss exakt mit dem Namespace-Namen auf Ihrem EKS Amazon-Cluster übereinstimmen.
   - Um einen Namespace zu entfernen, wählen Sie Entfernen neben dem Namespace.
   - Um die ausgewählten Namespaces auf alle EKS Amazon-Cluster anzuwenden, wählen Sie Namespaces auf alle Cluster anwenden. EKS

     Wenn Sie diese Option wählen, wird Ihre vorherige Namespace-Auswahl in den anderen EKS Amazon-Clustern durch die aktuelle Namespace-Auswahl überschrieben.
4. Um die aktualisierten Namespaces in Ihre Anwendung aufzunehmen, wählen Sie Aktualisieren.

Next

Schritt 4: Stellen Sie ein und RTO RPO

Schritt 4: Stellen Sie ein und RTO RPO

Sie können eine neue Resilienzrichtlinie mit Ihren eigenen RTO RPO /-Zielen definieren, oder Sie können eine bestehende Resilienzrichtlinie mit vordefinierten RTO RPO /-Zielen auswählen. Wenn Sie eine der vorhandenen Resilienzrichtlinien verwenden möchten, wählen Sie die Option Vorhandene Richtlinie auswählen und wählen Sie eine vorhandene Zielanwendung aus der Dropdownliste Optionselement aus.

Um Ihre eigenen RTO RPO /Ziele zu definieren

1. Wählen Sie die Option Neue Resilienzrichtlinie erstellen aus.
2. Geben Sie einen Namen für die Resilienzrichtlinie ein.
3. (Optional) Geben Sie eine Beschreibung für die Resilienzrichtlinie ein.
4. Definieren Sie Ihre RTO RTO/RPOim Bereich RPO /-Ziele.

   > **Note**
   >
   > - Wir haben einen Standard RTO und RPO für Ihre Anwendung ausgefüllt. Sie können das RTO und RPO jetzt ändern, oder nachdem Sie die Bewerbung geprüft haben.
   > - AWS Resilience Hub ermöglicht es Ihnen, den Wert Null in die RPOFelder RTOund Ihrer Resilienzrichtlinie einzugeben. Bei der Bewertung Ihrer Anwendung liegt das niedrigstmögliche Bewertungsergebnis jedoch nahe Null. Wenn Sie also in die RPOFelder RTOund den Wert Null eingeben, liegen die geschätzte Arbeitslast RTO und die geschätzten RPO Workload-Ergebnisse nahe Null, und der Compliance-Status für Ihre Anwendung wird auf Policy Breached gesetzt.

5. UmRTO/RPOfür Ihre Infrastruktur und AZ zu definieren, klicken Sie auf den Rechtspfeil, um den RPO Bereich Infrastruktur RTO und zu erweitern.
6. Geben Sie im Feld RTO/RPOtargets einen numerischen Wert in das Feld ein und wählen Sie dann die Zeiteinheit aus, die der Wert RTOsowohl für als auch darstellt RPO.

   Wiederholen Sie diese Einträge für Infrastruktur und Availability Zone im Bereich Infrastruktur RTO und RPO Availability Zone.

7. (Optional) Wenn Sie über eine Anwendung mit mehreren Regionen verfügen und eine Region RTO definieren möchtenRPO, aktivieren Sie die Option Region — optional.

   Geben Sie im Feld RTOund RPOeinen numerischen Wert in das Feld ein und wählen Sie dann die Zeiteinheit aus, für die der Wert RTOsowohl RPOals auch steht.

Next

the section called “Schritt 5: Richten Sie eine geplante Bewertung und eine Drift-Benachrichtigung ein”

Schritt 5: Richten Sie geplante Assessments und Drift-Benachrichtigungen ein

AWS Resilience Hub ermöglicht es Ihnen, geplante Bewertungen und Benachrichtigungen über Abweichungen einzurichten, um Ihre Anwendung täglich zu überprüfen und benachrichtigt zu werden, wenn eine Abweichung festgestellt wird.

So richten Sie die Benachrichtigung über Abweichungen ein

1. Um Ihre Bewerbung täglich zu bewerten, aktivieren Sie die Option „Täglich automatisch bewerten“.

   Wenn diese Option aktiviert ist, beginnt der Zeitplan für die tägliche Prüfung erst nach den folgenden Ereignissen:

   - Die Anwendung wird zum ersten Mal erfolgreich manuell geprüft.
   - Die Anwendung ist mit einer geeigneten IAM Rolle konfiguriert.
   - Wenn Ihre Anwendung mit aktuellen IAM Benutzerberechtigungen konfiguriert ist, müssen Sie die `AWSResilienceHubAsssessmentExecutionPolicy`

     Rolle unter Verwendung des entsprechenden Verfahrens inthe section called “Wie funktioniert AWS Resilience Hub mit IAM”.
2. Um benachrichtigt zu werden, wenn Abweichungen von den Resilienzrichtlinien AWS Resilience Hub erkannt werden oder wenn Ressourcen verschwendet werden, aktivieren Sie die Option Bei Änderungen der Anwendung benachrichtigen lassen.

Wenn diese Option aktiviert ist, müssen Sie ein Amazon Simple Notification Service (AmazonSNS) -Thema angeben, um Drift-Benachrichtigungen zu erhalten. Um ein SNS Amazon-Thema anzugeben, wählen Sie im Abschnitt SNS Thema angeben die Option SNSThema auswählen und wählen Sie ein SNS Amazon-Thema aus der Dropdownliste SNSThema auswählen aus.

> **Note**
>
> - Damit Sie Benachrichtigungen AWS Resilience Hub zu Ihren SNS Amazon-Themen veröffentlichen können, muss Ihr SNS Amazon-Thema mit den entsprechenden Berechtigungen konfiguriert sein. Weitere Informationen zur Konfiguration von Berechtigungen finden Sie unterthe section called “Aktivierung AWS Resilience Hub der Veröffentlichung in Ihren SNS Amazon-Themen”.
> - Tägliche Bewertungen können sich auf Ihr Kontingent an Durchläufen auswirken. Weitere Informationen zu Kontingenten finden Sie unter AWS Resilience Hub Endpunkte und Kontingente in der AWS Allgemeinen Referenz.

Um SNS Amazon-Themen zu verwenden, die sich in einer anderen AWS-Konto oder einer anderen Region oder in beiden befinden, wählen Sie SNSThema eingeben ARN und geben Sie den Amazon-Ressourcennamen (ARN) des SNS Amazon-Themas in das Feld SNSThema angeben ein. Weitere Informationen zu ARNs finden Sie unter Amazon Resource Names (ARNs) in der AWS Allgemeinen Referenz.

Next

Schritt 6: Berechtigungen einrichten

Schritt 6: Berechtigungen einrichten

AWS Resilience Hub ermöglicht es Ihnen, die erforderlichen Berechtigungen für das primäre Konto und das sekundäre Konto zu konfigurieren, um die Ressourcen zu ermitteln und zu bewerten. Sie müssen das Verfahren jedoch separat ausführen, um die Berechtigungen für jedes Konto zu konfigurieren.

Um IAM Rollen und IAM Berechtigungen zu konfigurieren

1. Um eine bestehende IAM Rolle auszuwählen, die für den Zugriff auf Ressourcen im aktuellen Konto verwendet werden soll, wählen Sie eine IAM Rolle aus der Dropdownliste IAMRolle auswählen aus.

   > **Note**
   >
   > Wenn Sie bei einer kontoübergreifenden Einrichtung die Amazon-Ressourcennamen (ARNs) der IAM Rolle nicht im ARN Feld Geben Sie eine IAM Rolle ein angeben, AWS Resilience Hub wird die IAM Rolle verwendet, die Sie aus der Dropdownliste IAMRolle auswählen ausgewählt haben, für alle Konten.

   Wenn Ihrem Konto noch keine IAM Rollen zugeordnet sind, können Sie mithilfe einer der folgenden Optionen eine IAM Rolle erstellen:

   - AWS IAMKonsole — Wenn Sie diese Option wählen, müssen Sie das Verfahren unter So erstellen Sie Ihre AWS Resilience Hub-Rolle in der IAM Konsole ausführen.
   - AWS CLI— Wenn Sie diese Option wählen, müssen Sie alle unter aufgeführten Schritte ausführen AWS CLI.
   - CloudFormation Vorlage — Wenn Sie diese Option wählen, müssen Sie je nach Kontotyp (primäres Konto oder sekundäres Konto) die Rollen anhand der entsprechenden AWS CloudFormation Vorlage erstellen.
2. Klicken Sie auf den Rechtspfeil, um den Abschnitt IAMRolle (n) aus einem kontoübergreifenden Konto hinzufügen — Optional zu erweitern.
3. Um IAM Rollen aus einem Cross-Konto auszuwählen, geben Sie die IAM Rolle ARNs der Rolle in das ARN Feld Geben Sie eine IAM Rolle ein. Vergewissern Sie sich, dass die ARNs von Ihnen eingegebene IAM Rolle nicht zum aktuellen Konto gehört.
4. Wenn Sie den aktuellen IAM Benutzer verwenden möchten, um Ihre Anwendungsressourcen zu ermitteln, klicken Sie auf den Rechtspfeil, um den Abschnitt Aktuelle IAM Benutzerberechtigungen verwenden zu erweitern, und wählen Sie Ich verstehe, dass ich die Berechtigungen manuell konfigurieren muss, um die darin enthaltenen Funktionen zu aktivieren AWS Resilience Hub.

Wenn Sie diese Option auswählen, funktionieren einige AWS Resilience Hub Funktionen (z. B. die Benachrichtigung über Abweichungen) möglicherweise nicht wie erwartet und die Eingaben, die Sie in Schritt 1 und Schritt 3 eingegeben haben, werden ignoriert.

Next

Schritt 7: Konfigurieren Sie die Konfigurationsparameter der Anwendung

Schritt 7: Konfigurieren Sie die Konfigurationsparameter der Anwendung

In diesem Abschnitt können Sie die Einzelheiten Ihres regionsübergreifenden Failover-Supports mithilfe von angeben. AWS Elastic Disaster Recovery AWS Resilience Hub verwendet diese Informationen, um Empfehlungen zur Ausfallsicherheit abzugeben.

Weitere Hinweise zu den Konfigurationsparametern von Anwendungen finden Sie unterKonfigurationsparameter der Anwendung.

So fügen Sie Anwendungskonfigurationsparameter hinzu (optional)

1. Um den Abschnitt Anwendungskonfigurationsparameter zu erweitern, wählen Sie den Rechtspfeil.
2. Geben Sie die Failover-Konto-ID in das Feld Konto-ID ein. Standardmäßig haben wir dieses Feld mit Ihrer Konto-ID, die für AWS Resilience Hub verwendet wird, vorausgefüllt. Diese kann geändert werden.
3. Wählen Sie eine Failover-Region aus der Dropdownliste Region aus.

> **Note**
>
> Wenn Sie diese Funktion deaktivieren möchten, wählen Sie "—" aus der Dropdownliste aus.

Next

Schritt 8: Fügen Sie Tags hinzu

Schritt 8: Fügen Sie Tags hinzu

Weisen Sie einer AWS Ressource ein Tag oder eine Bezeichnung zu, um Ihre Ressourcen zu suchen und zu filtern oder Ihre AWS Kosten zu verfolgen.

(Optional) Um Ihrer Anwendung Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen aus, wenn Sie der Anwendung ein oder mehrere Tags zuordnen möchten. Weitere Informationen zu Tags finden Sie unter Ressourcen taggen in der AWS allgemeinen Referenz.

Wählen Sie Anwendung hinzufügen, um Ihre Anwendung zu erstellen.

Next

Schritt 9: Überprüfe und veröffentliche deine AWS Resilience Hub Bewerbung

Schritt 9: Überprüfe und veröffentliche deine AWS Resilience Hub Bewerbung

Nach der Veröffentlichung können Sie die Anwendung weiterhin überprüfen und ihre Ressourcen bearbeiten. Wenn Sie fertig sind, wählen Sie Veröffentlichen, um die Anwendung zu veröffentlichen.

Weitere Informationen zur Überprüfung der Anwendung und zur Bearbeitung der zugehörigen Ressourcen finden Sie im Folgenden:

- the section called “Zusammenfassung der Anwendung anzeigen”
- the section called “Anwendungsressourcen bearbeiten”

Next

Schritt 10: Führen Sie eine Bewertung Ihrer AWS Resilience Hub Bewerbung durch

Schritt 10: Führen Sie eine Bewertung Ihrer AWS Resilience Hub Bewerbung durch

Die Anwendung, die Sie veröffentlicht haben, ist auf der Übersichtsseite aufgeführt.

Nachdem Sie Ihre AWS Resilience Hub Anwendung veröffentlicht haben, werden Sie auf die Seite mit der Anwendungsübersicht weitergeleitet, auf der Sie eine Resilienzbewertung durchführen können. Bei der Bewertung wird Ihre Anwendungskonfiguration anhand der Resilienzrichtlinie

bewertet, die Ihrer Anwendung zugeordnet ist. Es wird ein Bewertungsbericht erstellt, aus dem hervorgeht, wie Ihre Anwendung im Hinblick auf die Ziele Ihrer Ausfallsicherheitsrichtlinie abschneidet.

Um eine Resilienzbewertung durchzuführen

1. Wählen Sie auf der Seite mit der Anwendungsübersicht die Option Resiliency bewerten aus.
2. Geben Sie im Dialogfeld Resilienzbewertung ausführen einen eindeutigen Namen für den Bericht ein, oder verwenden Sie den generierten Namen im Feld Berichtsname.
3. Wählen Sie Ausführen aus.
4. Nachdem Sie darüber informiert wurden, dass der Bewertungsbericht generiert wurde, wählen Sie die Registerkarte Bewertungen und wählen Sie Ihre Bewertung aus, um den Bericht anzuzeigen.
5. Wählen Sie den Tab Prüfen, um den Bewertungsbericht Ihrer Bewerbung einzusehen.

Verwenden AWS Resilience Hub

AWS Resilience Hub hilft Ihnen, die Ausfallsicherheit Ihrer Anwendungen zu verbessern AWS und die Wiederherstellungszeit bei Anwendungsausfällen zu verkürzen.

Themen:

AWS Resilience Hub Armaturenbrett

Das Dashboard bietet einen umfassenden Überblick über den Resilienzstatus Ihres Anwendungsportfolios. Das Dashboard aggregiert und organisiert Ausfallsicherheitsereignisse (z. B. nicht verfügbare Datenbank oder fehlgeschlagene Resilienzvalidierung), Warnmeldungen und Erkenntnisse von Services wie CloudWatch Amazon Fault Injection Service (AWS FIS).

Das Dashboard generiert außerdem einen Resilienz-Score für jede bewertete Anwendung. Diese Bewertung gibt an, wie gut Ihre Anwendung abschneidet, wenn sie anhand von empfohlenen Stabilitätsrichtlinien, Alarmen, Standardarbeitsanweisungen (SOPs) für die Wiederherstellung und Tests bewertet wird. Sie können diesen Wert verwenden, um die Verbesserung der Ausfallsicherheit im Laufe der Zeit zu messen.

Um das AWS Resilience Hub Dashboard anzuzeigen, wählen Sie Dashboard aus dem Navigationsmenü. Auf der Dashboard-Seite werden die folgenden Abschnitte angezeigt:

Status der Bewerbung

Der Status der Anträge gibt an, ob die Anwendungen auf ihre Einhaltung der jeweiligen Ausfallsicherheitsrichtlinie geprüft wurden oder nicht. Darüber hinaus gibt der Status nach Abschluss

einer Bewertung auch an, ob die Eingabequellen Ihrer Anwendungen geändert wurden oder nicht. Wählen Sie unter jedem der folgenden Status eine Zahl aus, um alle Bewerbungen mit demselben Status auf der Seite „Bewerbungen“ anzuzeigen:

- Anwendungen in der Richtlinie — Zeigt alle Anwendungen an, die die jeweilige Resilienzrichtlinie einhalten.
- Anwendungen, die gegen die Richtlinien verstoßen — Weist auf alle Anwendungen hin, die die ihnen zugeordnete Ausfallsicherheitsrichtlinie nicht einhalten.
- Nicht bewertete Anwendungen — Zeigt alle Anwendungen an, deren Konformität noch nicht bewertet oder nachverfolgt wurde.
- Anwendungen drifteten — Zeigt alle Anwendungen an, die ihre Stabilitätsrichtlinie nicht eingehalten haben oder ob ihre Ressourcen abgewichen sind.

Bewertung der Ausfallsicherheit von Anwendungen im Laufe der Zeit

Anhand der Bewertung der Anwendungsausfallsicherheit im Zeitverlauf können Sie sich ein Diagramm der Ausfallsicherheit Ihrer Anwendung in den letzten 30 Tagen anzeigen lassen. Das Dropdownmenü kann zwar 10 Ihrer Anwendungen auflisten, zeigt Ihnen jedoch AWS Resilience Hub nur ein Diagramm von bis zu vier Anwendungen gleichzeitig. Weitere Informationen zur Resilienzbewertung finden Sie unter. Resilienzwerte verstehen

> **Note**
>
> AWS Resilience Hub führt geplante Bewertungen nicht gleichzeitig durch. Daher müssen Sie möglicherweise zu einem späteren Zeitpunkt zum Diagramm der Resilienzbewertung im Zeitverlauf zurückkehren, um die tägliche Bewertung Ihrer Anwendungen einzusehen.

AWS Resilience Hub verwendet Amazon auch CloudWatch , um diese Grafiken zu generieren. Wählen Sie Metriken anzeigen in CloudWatch, um detailliertere Informationen zur Ausfallsicherheit Ihrer Anwendung in Ihrem CloudWatch Dashboard zu erstellen und anzuzeigen. Weitere Informationen CloudWatch dazu finden Sie unter Verwenden von Dashboards im CloudWatch Amazon-Benutzerhandbuch.

Alarme wurden implementiert

In diesem Abschnitt sind alle Alarme aufgeführt, die Sie in Amazon eingerichtet haben CloudWatch , um alle Anwendungen zu überwachen. Weitere Informationen finden Sie unter Alarme anzeigen.

Durchgeführte Experimente

In diesem Abschnitt werden alle Experimente zur Fehlerinjektion aufgeführt, die Sie in allen Anwendungen implementiert haben. Weitere Informationen finden Sie unter Experimente mit Fehlerinjektion anzeigen.

AWS Resilience Hub Anwendungen beschreiben und verwalten

Eine AWS Resilience Hub Anwendung ist eine Sammlung von AWS Ressourcen, die so strukturiert sind, dass sie AWS Anwendungsunterbrechungen verhindern und beheben.

Um eine AWS Resilience Hub Anwendung zu beschreiben, geben Sie einen Anwendungsnamen, Ressourcen aus einem oder mehreren AWS CloudFormation Stacks und eine entsprechende Ausfallsicherheitsrichtlinie an. Sie können auch jede vorhandene AWS Resilience Hub Anwendung als Vorlage für die Beschreibung Ihrer Anwendung verwenden.

Nachdem Sie eine AWS Resilience Hub Anwendung beschrieben haben, müssen Sie sie veröffentlichen, damit Sie eine Resilienzbewertung für sie durchführen können. Anschließend können Sie die Empfehlungen aus der Bewertung verwenden, um die Ausfallsicherheit zu verbessern, indem Sie eine weitere Bewertung durchführen, die Ergebnisse vergleichen und den Vorgang dann wiederholen, bis Ihre geschätzte Arbeitslast RTO und die geschätzte Arbeitslast Ihren RPO RTO Zielvorgaben entsprechen. RPO

Um die Seite Anwendungen aufzurufen, wählen Sie im Navigationsbereich Anwendungen aus. Sie können Ihre Anwendungen auf der Seite „Anwendungen“ wie folgt identifizieren:

- Name — Der Name der Anwendung, die Sie bei der Definition angegeben haben AWS Resilience Hub.
- Beschreibung — Die Beschreibung der Anwendung, die Sie bei der Definition angegeben haben AWS Resilience Hub.
- Konformitätsstatus — AWS Resilience Hub legt den Anwendungsstatus auf „Bewertet“, „Nicht bewertet“, „Richtlinie verletzt“ oder „Änderungen erkannt“ fest.

  - Beurteilt — AWS Resilience Hub hat Ihre Bewerbung bewertet.
  - Nicht bewertet — AWS Resilience Hub hat Ihre Bewerbung nicht bewertet.
  - Verstoß gegen die Richtlinie — es AWS Resilience Hub wurde festgestellt, dass Ihre Anwendung die in Ihrer Stabilitätsrichtlinie festgelegten Ziele für Recovery Time Objective (RTO) und Recovery Point Objective () nicht erfüllt hat. RPO Lesen Sie die Empfehlungen von und verwenden Sie sie, AWS Resilience Hub bevor Sie Ihre Anwendung im Hinblick auf die Ausfallsicherheit neu bewerten. Weitere Informationen zu Empfehlungen finden Sie unter. Fügen Sie eine Anwendung hinzu zu AWS Resilience Hub
  - Änderungen erkannt — AWS Resilience Hub hat Änderungen an der mit Ihrer Anwendung verknüpften Ausfallsicherheitsrichtlinie festgestellt. Sie müssen Ihre Anwendung erneut bewerten AWS Resilience Hub , um festzustellen, ob Ihre Anwendung die Ziele Ihrer Ausfallsicherheitsrichtlinie erfüllt.
- Geplante Bewertungen — Der Ressourcentyp identifiziert die Komponentenressource für Ihre Anwendung. Weitere Informationen zu geplanten Assessments finden Sie unterAusfallsicherheit von Anwendungen.
  - Aktiv — Dies bedeutet, dass Ihre Bewerbung täglich automatisch von geprüft wird AWS Resilience Hub.
  - Deaktiviert — Dies bedeutet, dass Ihre Bewerbung nicht automatisch täglich von geprüft wird AWS Resilience Hub und Sie Ihre Bewerbung manuell prüfen müssen.
- Drift-Status — Zeigt an, ob Ihre Bewerbung von der vorherigen erfolgreichen Prüfung abweicht oder nicht, und legt einen der folgenden Status fest:
  - Drifted — Weist darauf hin, dass die Anwendung, die bei der vorherigen erfolgreichen Bewertung ihre Resilienz-Richtlinie eingehalten hat, nun gegen die Resilienz-Richtlinie verstoßen hat und die Anwendung gefährdet ist. Darüber hinaus wird angegeben, ob die Ressourcen in den Eingabequellen, die in der aktuellen Anwendungsversion enthalten sind, hinzugefügt oder entfernt wurden.
  - Nicht verändert — Zeigt an, dass die Anwendung weiterhin voraussichtlich ihre RTO und die in der Richtlinie definierten RPO Ziele erreicht. Darüber hinaus weist es auch darauf hin, dass die Ressourcen in den Eingabequellen, die in der aktuellen Anwendungsversion enthalten sind, nicht hinzugefügt oder entfernt wurden.
- Geschätzte Arbeitslast RTO — Gibt die maximal mögliche geschätzte Arbeitslast RTO Ihrer Anwendung an. Dieser Wert ist die geschätzte maximale Arbeitslast RTO aller Störungstypen aus der letzten erfolgreichen Bewertung.

- Geschätzte Arbeitslast RPO — Gibt die maximal mögliche geschätzte Arbeitslast RPO Ihrer Anwendung an. Dieser Wert ist die geschätzte maximale Arbeitslast RTO aller Störungstypen aus der letzten erfolgreichen Bewertung.
- Uhrzeit der letzten Prüfung — Gibt das Datum und die Uhrzeit an, zu der Ihre Anwendung zuletzt erfolgreich geprüft wurde.
- Erstellungszeit — Datum und Uhrzeit der Erstellung der Anwendung.
- ARN— Der Amazon-Ressourcenname (ARN) Ihrer Anwendung. Weitere Informationen zu ARNs finden Sie unter Amazon Resource Names (ARNs) in der AWS Allgemeinen Referenz.

> **Note**
>
> AWS Resilience Hub kann die Resilienz regionsübergreifender ECS Amazon-Ressourcen nur dann vollständig beurteilen, wenn Sie Amazon ECR für das Image-Repository verwenden.

Darüber hinaus können Sie die Anwendungsliste auch filtern, indem Sie eine der folgenden Optionen auf der Anwendungsseite verwenden:

- Anwendungen suchen — Geben Sie Ihren Anwendungsnamen ein, um die Ergebnisse nach dem Namen Ihrer Anwendung zu filtern.
- Uhrzeit der letzten Prüfung nach Datum und Zeitraum filtern — Um diesen Filter anzuwenden, klicken Sie auf das Kalendersymbol und wählen Sie eine der folgenden Optionen, um nach den Ergebnissen zu filtern, die dem Zeitraum entsprechen:
  - Relativer Bereich — Wählen Sie eine der verfügbaren Optionen aus und klicken Sie auf Anwenden.

    Wenn Sie die Option Benutzerdefinierter Bereich wählen, geben Sie eine Dauer in das Feld Dauer eingeben ein, wählen Sie die entsprechende Zeiteinheit aus der Dropdownliste Zeiteinheit aus und wählen Sie dann Anwenden.
  - Absoluter Bereich — Um das Datum und den Zeitraum festzulegen, geben Sie die Start- und Endzeit an und wählen Sie dann Anwenden.

In den folgenden Themen werden die verschiedenen Ansätze zur Beschreibung einer AWS Resilience Hub Anwendung und deren Verwaltung beschrieben.

Themen

Zusammenfassung einer AWS Resilience Hub Anwendung anzeigen

Die Seite mit der Anwendungsübersicht in der AWS Resilience Hub Konsole bietet einen Überblick über Ihre Anwendungsinformationen und den Zustand der Ausfallsicherheit.

Um eine Anwendungszusammenfassung anzuzeigen

1. Wählen Sie im Navigationsbereich Anwendungen aus.
2. Wählen Sie auf der Seite „Anwendungen“ den Namen der Anwendung aus, die Sie anzeigen möchten.

Die Seite mit der Zusammenfassung der Anwendungen besteht aus den folgenden Abschnitten.

Themen

Zusammenfassung der Bewertung

Dieser Abschnitt enthält eine Zusammenfassung der letzten erfolgreichen Bewertung und hebt wichtige Empfehlungen als umsetzbare Erkenntnisse hervor. AWS Resilience Hub verwendet die

generativen KI-Funktionen von Amazon Bedrock, um Benutzern zu helfen, sich auf die wichtigsten Resilienz-Empfehlungen von AWS Resilience Hub zu konzentrieren. Indem Sie sich auf die wichtigsten Punkte konzentrieren, können Sie sich auf die wichtigsten Empfehlungen konzentrieren, die die Ausfallsicherheit Ihrer Anwendung verbessern. Wählen Sie eine Empfehlung aus, um deren Zusammenfassung anzuzeigen, und klicken Sie auf Details anzeigen, um weitere Einzelheiten zu den Empfehlungen im entsprechenden Abschnitt des Bewertungsberichts anzuzeigen. Weitere Informationen zur Überprüfung des Bewertungsberichts finden Sie unterthe section called "Überprüfung der Bewertungsberichte".

> **Note**
>
> - Diese Bewertungszusammenfassung ist nur in der Region USA Ost (Nord-Virginia) verfügbar.
> - Die von großen Sprachmodellen (LLMs) auf Amazon Bedrock generierten Bewertungszusammenfassungen sind nur Vorschläge. Der aktuelle Stand der generativen KI-Technologie ist nicht perfekt und nicht LLMs unfehlbar. Vorurteile und falsche Antworten sind zwar selten, sollten aber erwartet werden. Prüfen Sie jede Empfehlung in der Bewertungszusammenfassung, bevor Sie die Ergebnisse eines verwendenLLM.

Übersicht

Dieser Abschnitt enthält eine Zusammenfassung der ausgewählten Anwendung in den folgenden Abschnitten:

- Anwendungsinformationen — Dieser Abschnitt enthält die folgenden Informationen zur ausgewählten Anwendung:
  - Bewerbungsstatus — Zeigt den Status der Bewerbung an.
  - Beschreibung — Die Beschreibung der Anwendung.
  - Version — Gibt die aktuell getestete Version der Anwendung an.
  - Ausfallsicherheitsrichtlinie — Gibt die Ausfallsicherheitsrichtlinie an, die der Anwendung zugeordnet ist. Weitere Informationen zu Resilienzrichtlinien finden Sie unter. Verwaltung von Resilienzrichtlinien
- Anwendungsabweichungen — In diesem Abschnitt werden die Abweichungen hervorgehoben, die bei der Durchführung einer Bewertung der ausgewählten Anwendung festgestellt wurden, um zu überprüfen, ob sie mit ihrer Ausfallsicherheitsrichtlinie konform ist. Darüber hinaus wird geprüft, ob

Ressourcen seit der letzten Veröffentlichung der Anwendungsversion hinzugefügt oder entfernt wurden. In diesem Abschnitt werden die folgenden Informationen angezeigt:

- Richtlinienabweichungen — Wählen Sie die unten stehende Zahl aus, um alle Anwendungskomponenten anzuzeigen, die der Richtlinie in der vorherigen Bewertung, aber in der aktuellen Bewertung nicht entsprachen.
- Ressourcenabweichungen — Wählen Sie die unten stehende Zahl aus, um alle ungenutzten Ressourcen in der letzten Bewertung zu sehen.

Ausfallsicherheit von Anwendungen

Die im Abschnitt Resilienzbewertung angegebenen Kennzahlen stammen aus der letzten Resilienzbewertung der Anwendung.

Resilienz-Punktzahl

Der Resiliency Score hilft Ihnen dabei, Ihre Bereitschaft zu quantifizieren, mit einer potenziellen Störung umzugehen. Diese Bewertung gibt an, wie genau Ihre Anwendung die AWS Resilience Hub Empfehlungen zur Einhaltung der Stabilitätsrichtlinien, Alarme, Standardarbeitsanweisungen (SOPs) und Tests der Anwendung befolgt hat.

Der maximale Stabilitätswert, den Ihre Anwendung erreichen kann, liegt bei 100%. Die Punktzahl steht für alle empfohlenen Tests, die in einem vordefinierten Zeitraum ausgeführt werden. Es zeigt an, dass die Tests den richtigen Alarm auslösen und dass der Alarm den richtigen auslöst. SOP

Nehmen wir zum Beispiel an, dass ein Test mit einem Alarm und einem AWS Resilience Hub empfohlen wird. SOP Wenn der Test ausgeführt wird, löst der Alarm den zugehörigen SOP aus und wird dann erfolgreich ausgeführt. Weitere Informationen zur Resilienzbewertung finden Sie unter. Resilienzwerte verstehen

Alarme wurden implementiert

Im Abschnitt Implementierte Alarme der Anwendung werden die Alarme aufgeführt, die Sie in Amazon eingerichtet haben CloudWatch , um die Anwendung zu überwachen. Weitere Informationen zu Alarmen finden Sie unterVerwalten von Alarmen.

Experimente wurden durchgeführt

Der Abschnitt Fehlerinjektionsexperimente mit Zusammenfassung der Anwendung enthält eine Liste der Fehlerinjektionsexperimente. Weitere Informationen zu Experimenten mit Fehlerinjektion finden Sie unterVerwaltung von Amazon Fault Injection Service-Experimenten.

AWS Resilience Hub Anwendungsressourcen bearbeiten

Um genaue und hilfreiche Resilienzbeurteilungen zu erhalten, stellen Sie sicher, dass Ihre Anwendungsbeschreibung aktualisiert ist und mit Ihrer tatsächlichen AWS Anwendung und Ihren Ressourcen übereinstimmt. Bewertungsberichte, Validierungen und Empfehlungen basieren auf den aufgeführten Ressourcen. Wenn Sie Ressourcen zu einer AWS Anwendung hinzufügen oder daraus entfernen, sollten Sie diese Änderungen in berücksichtigen AWS Resilience Hub.

AWS Resilience Hub sorgt für Transparenz über Ihre Anwendungsquellen. Sie können die Ressourcen und Anwendungsquellen in Ihrer Anwendung identifizieren und bearbeiten.

> **Note**
>
> Durch die Bearbeitung der Ressourcen wird nur die AWS Resilience Hub Referenz Ihrer Anwendung geändert. An Ihren tatsächlichen Ressourcen werden keine Änderungen vorgenommen.

Sie können fehlende Ressourcen hinzufügen, vorhandene Ressourcen ändern oder Ressourcen entfernen, die Sie nicht benötigen. Ressourcen sind in logische Anwendungskomponenten (AppComponents) gruppiert. Sie können die bearbeiten AppComponents , um die Struktur Ihrer Anwendung besser widerzuspiegeln.

Erweitern oder aktualisieren Sie Ihre Anwendungsressourcen, indem Sie eine Entwurfsversion Ihrer Anwendung bearbeiten und die Änderungen in einer neuen (Release-) Version veröffentlichen. AWS Resilience Hub verwendet die Release-Version (die die aktualisierten Ressourcen enthält) Ihrer Anwendung für die Durchführung von Resilienzanalysen.

Um die Ausfallsicherheit Ihrer Anwendung zu bewerten

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen den Namen der Anwendung aus, die Sie bearbeiten möchten.

3. Wählen Sie im Menü Aktionen die Option Resilienz bewerten aus.
4. Geben Sie im Dialogfeld Resilienzbewertung ausführen einen eindeutigen Namen für den Bericht ein, oder verwenden Sie den generierten Namen im Feld Berichtsname.
5. Wählen Sie Ausführen aus.
6. Nachdem Sie darüber informiert wurden, dass der Bewertungsbericht generiert wurde, wählen Sie die Registerkarte Bewertungen und wählen Sie Ihre Bewertung aus, um den Bericht anzuzeigen.
7. Wählen Sie den Tab Prüfen, um den Bewertungsbericht Ihrer Bewerbung einzusehen.

Um die geplante Bewertung zu aktivieren

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen die Anwendung aus, für die Sie die geplante Bewertung aktivieren möchten.
3. Aktivieren Sie die Option „Täglich automatisch bewerten“.

Um die geplante Bewertung zu deaktivieren

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen die Anwendung aus, für die Sie die geplante Bewertung aktivieren möchten.
3. Deaktivieren Sie die Option „Täglich automatisch bewerten“.

> **Note**
>
> Wenn Sie die geplante Bewertung deaktivieren, wird die Benachrichtigung über Abweichungen deaktiviert.

4. Wählen Sie Ausschalten.

Um die Drift-Benachrichtigung für Ihre Anwendung zu aktivieren

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).

2. Wählen Sie auf der Seite Anwendungen die Anwendung aus, für die Sie die Drift-Benachrichtigung aktivieren möchten, oder bearbeiten Sie die Einstellungen für Drift-Benachrichtigungen.
3. Sie können die Drift-Benachrichtigung bearbeiten, indem Sie eine der folgenden Optionen wählen:
   - Wählen Sie unter Aktionen die Option Drift-Benachrichtigung aktivieren aus.
   - Wählen Sie im Abschnitt Anwendungsabweichungen die Option Benachrichtigung aktivieren aus.
4. Führen Sie die unter beschriebenen Schritte ausSchritt 5: Richten Sie geplante Assessments und Drift-Benachrichtigungen ein, und kehren Sie dann zu diesem Verfahren zurück.
5. Wählen Sie Enable (Aktivieren) aus.

   Wenn Sie die Drift-Benachrichtigung aktivieren, können Sie auch eine geplante Bewertung durchführen.

Um die Drift-Benachrichtigung für Ihre Anwendung zu bearbeiten

> **Note**
>
> Dieses Verfahren ist anwendbar, wenn Sie die Option „Geplante Prüfung“ (die Option „Automatisch täglich bewerten“ ist aktiviert) und die Benachrichtigung über Abweichungen aktiviert haben.

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen die Anwendung aus, für die Sie die Drift-Benachrichtigung aktivieren oder die Einstellungen für Drift-Benachrichtigungen bearbeiten möchten.
3. Sie können die Drift-Benachrichtigung bearbeiten, indem Sie eine der folgenden Optionen wählen:
   - Wählen Sie unter Aktionen die Option Drift-Benachrichtigung bearbeiten aus.
   - Wählen Sie im Abschnitt Anwendungsabweichungen die Option Benachrichtigung bearbeiten aus.

4. Führen Sie die Schritte unter ausSchritt 5: Richten Sie geplante Assessments und Drift-Benachrichtigungen ein, und kehren Sie dann zu diesem Verfahren zurück.
5. Wählen Sie Speichern.

Um die Sicherheitsberechtigungen Ihrer Anwendung zu aktualisieren

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen die Anwendung aus, für die Sie die Sicherheitsberechtigungen aktualisieren möchten.
3. Wählen Sie unter Aktionen die Option Berechtigungen aktualisieren aus.
4. Um die Sicherheitsberechtigungen zu aktualisieren, führen Sie die Schritte unter ausSchritt 6: Berechtigungen einrichten, und kehren Sie dann zu diesem Verfahren zurück.
5. Wählen Sie Speichern und aktualisieren aus.

Um Ihrer Anwendung eine Ausfallsicherheitsrichtlinie hinzuzufügen

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen den Namen der Anwendung aus, die Sie bearbeiten möchten.
3. Wählen Sie im Menü Aktionen die Option Resilienzrichtlinie anhängen aus.
4. Wählen Sie im Dialogfeld „Richtlinie anhängen“ aus der Dropdownliste „Resilienzrichtlinie auswählen“ eine Resilienzrichtlinie aus.
5. Wählen Sie Anfügen aus.

Um Eingabequellen, Ressourcen und AppComponents Ihre Anwendung zu bearbeiten

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen den Namen der Anwendung aus, die Sie bearbeiten möchten.
3. Wählen Sie die Registerkarte Anwendungsstruktur.
4. Wählen Sie das Pluszeichen + vor Version und wählen Sie dann die Anwendungsversion mit dem Status Entwurf aus.
5. Gehen Sie wie folgt vor, um Eingabequellen, Ressourcen und AppComponents Ihre Anwendung zu bearbeiten.

Um die Eingabequellen Ihrer Anwendung zu bearbeiten

1. Um die Eingabequellen Ihrer Anwendung zu bearbeiten, wählen Sie die Registerkarte Eingabequellen.

   Im Abschnitt Eingabequellen werden alle Eingabequellen Ihrer Anwendungsressourcen aufgeführt. Sie können die Eingabequellen wie folgt identifizieren:

   - Quellenname — Der Name der Eingabequelle. Wählen Sie einen Quellnamen, um die zugehörigen Details in der jeweiligen Anwendung anzuzeigen. Für manuell hinzugefügte Eingabequellen ist der Link nicht verfügbar. Wenn Sie beispielsweise den Quellnamen wählen, der aus einem AWS CloudFormation Stack importiert wird, werden Sie auf die Seite mit den Stack-Details in der AWS CloudFormation Konsole weitergeleitet.
   - Quell-ARN — Der Amazon-Ressourcenname (ARN) der Eingabequelle. Wählen Sie einen ARN aus, um seine Details in der jeweiligen Anwendung anzuzeigen. Für manuell hinzugefügte Eingabequellen ist der Link nicht verfügbar. Wenn Sie beispielsweise einen ARN auswählen, der aus einem AWS CloudFormation Stack importiert wird, werden Sie auf die Seite mit den Stack-Details auf der AWS CloudFormation Konsole weitergeleitet.
   - Quelltyp — Der Typ der Eingabequelle. Zu den Eingabequellen gehören Amazon EKS-Cluster, AWS CloudFormation Stacks, AppRegistry Anwendungen AWS Resource Groups, Terraform-Statusdateien und manuell hinzugefügte Ressourcen.
   - Zugeordnete Ressourcen — Die Anzahl der Ressourcen, die der Eingabequelle zugeordnet sind. Wählen Sie eine Zahl, um alle zugehörigen Ressourcen einer Eingabequelle auf der Registerkarte Ressourcen anzuzeigen.
2. Um Ihrer Anwendung Eingabequellen hinzuzufügen, wählen Sie im Abschnitt Eingabequellen hinzufügen aus. Weitere Informationen zum Hinzufügen von Eingabequellen finden Sie unterthe section called “Schritt 3: Fügen Sie Ihrer AWS Resilience Hub Anwendung Ressourcen hinzu”.
3. Um Eingabequellen zu bearbeiten, wählen Sie die Eingabequellen aus und wählen Sie unter Aktionen eine der folgenden Optionen aus:

   - Eingabequellen erneut importieren (bis zu 5) — Importiert bis zu fünf ausgewählte Eingabequellen erneut.
   - Eingabequellen löschen — Löscht die ausgewählten Eingabequellen.

     Um eine Anwendung zu veröffentlichen, muss sie mindestens eine Eingabequelle enthalten. Wenn Sie alle Eingabequellen löschen, wird die Option Neue Version veröffentlichen deaktiviert.

Um die Ressourcen Ihrer Anwendung zu bearbeiten

1. Um die Ressourcen Ihrer Anwendung zu bearbeiten, wählen Sie die Registerkarte Ressourcen.

   > **Note**
   >
   > Um die Liste der nicht bewerteten Ressourcen anzuzeigen, wählen Sie „Nicht bewertete Ressourcen anzeigen“.

   Im Abschnitt Ressourcen werden Ressourcen aus der Anwendung aufgeführt, die Sie als Vorlage für Ihre Anwendungsbeschreibung verwenden möchten. Um Ihr Sucherlebnis zu verbessern, AWS Resilience Hub hat Ressourcen auf der Grundlage mehrerer Suchkriterien gruppiert. Zu diesen Suchkriterien gehören AppComponent Typen, Nicht unterstützte Ressourcen und Ausgeschlossene Ressourcen. Um die Ressourcen anhand eines Suchkriteriums in der Tabelle Ressourcen zu filtern, wählen Sie die Zahl unter den einzelnen Suchkriterien aus.

   Sie können die Ressourcen wie folgt identifizieren:

   - Logische ID — Eine logische ID ist ein Name, der verwendet wird, um Ressourcen in Ihrem AWS CloudFormation Stack, Ihrer Terraform-Statusdatei, Ihrer manuell hinzugefügten Anwendung, AppRegistry Anwendung oder zu identifizieren. AWS Resource Groups

     > **Note**
     >
     > - Mit Terraform können Sie denselben Namen für verschiedene Ressourcentypen verwenden. Daher sehen Sie am Ende der logischen ID für Ressourcen, die denselben Namen haben, "- Ressourcentyp".
     > - Um die Instanzen aller Anwendungsressourcen anzuzeigen, wählen Sie das Pluszeichen (+) vor der logischen ID. Um alle Instanzen einer Anwendungsressource anzuzeigen, wählen Sie das Pluszeichen (+) vor der logischen ID jeder Ressource.
     >
     > Weitere Informationen zu den unterstützten Ressourcen finden Sie unterthe section called “Unterstützte AWS Resilience Hub Ressourcen”.

- Ressourcentyp — Der Ressourcentyp identifiziert die Komponentenressource für Ihre Anwendung. `AWS::EC2::Instance`Deklariert beispielsweise eine Amazon EC2 EC2-Instance. Weitere Informationen zum Gruppieren von AppComponent Ressourcen finden Sie unter. Gruppieren von Ressourcen in einer Anwendungskomponente
- Quellname — Der Name der Eingabequelle. Wählen Sie einen Quellnamen, um die zugehörigen Details in der jeweiligen Anwendung anzuzeigen. Für manuell hinzugefügte Eingabequellen ist der Link nicht verfügbar. Wenn Sie beispielsweise den Quellnamen wählen, der aus einem AWS CloudFormation Stack importiert wird, werden Sie auf die Seite mit den Stack-Details auf der weitergeleitet AWS CloudFormation.
- Quelltyp — Der Typ der Eingabequelle. Zu den Eingabequellen gehören AWS CloudFormation Stapel, AppRegistry Anwendungen AWS Resource Groups, Terraform-Statusdateien und manuell hinzugefügte Ressourcen.

  > **Note**
  >
  > Um Ihre Amazon EKS-Cluster zu bearbeiten, führen Sie die Schritte unter So bearbeiten Sie die Eingabequellen Ihres AWS Resilience Hub Antragsverfahrens aus.

- Quellstapel — Der AWS CloudFormation Stapel, der die Ressource enthält. Diese Spalte hängt von der Art der Anwendungsstruktur ab, die Sie ausgewählt haben.
- Physikalische ID — Die tatsächlich zugewiesene Kennung für diese Ressource, z. B. eine Amazon EC2 EC2-Instance-ID oder ein S3-Bucket-Name.
- Inbegriffen — Gibt an, ob diese Ressourcen in der Anwendung AWS Resilience Hub enthalten sind.
- Bewertbar — Dies gibt an, ob Ihre Ressource im Hinblick auf ihre Widerstandsfähigkeit bewertet AWS Resilience Hub wird.
- AppComponents— Die AWS Resilience Hub Komponente, die dieser Ressource zugewiesen wurde, als ihre Anwendungsstruktur erkannt wurde.
- Name — Name der Anwendungsressource.
- Konto — Das AWS Konto, dem die physische Ressource gehört.

2. Um eine Ressource zu finden, die nicht aufgeführt ist, geben Sie die logische ID der Ressource in das Suchfeld ein.
3. Um eine Ressource aus Ihrer Anwendung zu entfernen, wählen Sie die Ressource aus und klicken Sie dann auf Ressource aus Aktionen ausschließen.
4. Um die Ressourcen in Ihrer Anwendung aufzulösen, wählen Sie Ressourcen aktualisieren aus.

5. Gehen Sie wie folgt vor, um Ihre vorhandenen Anwendungsressourcen zu ändern:

    a. Wählen Sie eine Ressource aus und klicken Sie dann unter Aktionen auf Stacks aktualisieren.

    b. Um Ihre Ressourcen zu aktualisieren, führen Sie auf der Seite Stacks aktualisieren die entsprechenden Verfahren unter ausSchritt 3: Fügen Sie Ihrer AWS Resilience Hub Anwendung Ressourcen hinzu, und kehren Sie dann zu diesem Verfahren zurück.

    c. Wählen Sie Speichern.

6. Um Ihrer Anwendung eine Ressource hinzuzufügen, wählen Sie unter Aktionen die Option Ressource hinzufügen aus und führen Sie die folgenden Schritte aus:

    a. Wählen Sie in der Dropdownliste Ressourcentyp einen Ressourcentyp aus.

    b. Wählen Sie einen AppComponent aus der AppComponentDrop-down-Liste aus.

    c. Geben Sie die logische ID der Ressource in das Feld Ressourcenname ein.

    d. Geben Sie die physische Ressourcen-ID oder den Ressourcennamen oder den Ressourcen-ARN in das Feld Ressourcen-ID ein.

    e. Wählen Sie Hinzufügen aus.

7. Um den Ressourcennamen zu bearbeiten, wählen Sie eine Ressource aus, wählen Sie unter Aktionen die Option Ressourcennamen bearbeiten aus, und führen Sie dann die folgenden Schritte aus:

    a. Geben Sie die logische ID der Ressource in das Feld Ressourcenname ein.

    b. Wählen Sie Speichern.

8. Um die Ressourcen-ID zu bearbeiten, wählen Sie eine Ressource aus, wählen Sie unter Aktionen die Option Ressourcen-ID bearbeiten aus und führen Sie dann die folgenden Schritte aus:

    a. Geben Sie die physische Ressourcen-ID oder den Ressourcennamen oder den Ressourcen-ARN in das Feld Ressourcen-ID ein.

    b. Wählen Sie Speichern.

9. Um die zu ändern AppComponent, wählen Sie eine Ressource aus, wählen Sie unter Aktionen die Option Ändern AppComponent aus und führen Sie die folgenden Schritte aus:

    a. Wählen Sie eine AppComponent aus der AppComponentDropdownliste aus.

    b. Wählen Sie Hinzufügen aus.

10. Um eine Ressource zu löschen, wählen Sie eine Ressource aus und klicken Sie dann unter Aktionen auf Ressource löschen.
11. Um eine Ressource einzubeziehen, wählen Sie eine Ressource aus und wählen Sie dann unter Aktionen die Option Ressource einbeziehen aus.

Um die AppComponents Ihrer Anwendung zu bearbeiten

1. Um Ihre Bewerbung zu bearbeiten, wählen Sie die AppComponentsRegisterkarte. AppComponents

   > **Note**
   >
   > Weitere Informationen zum Gruppieren von AppComponent Ressourcen finden Sie unterGruppieren von Ressourcen in einer Anwendungskomponente.

   AppComponentsIn diesem Abschnitt sind alle logischen Komponenten aufgeführt, in die die Ressourcen gruppiert sind. Sie können die AppComponents anhand der folgenden Merkmale identifizieren:

   - AppComponent Name — Der Name der AWS Resilience Hub Komponente, die dieser Ressource zugewiesen wurde, als ihre Anwendungsstruktur erkannt wurde.
   - AppComponent type — Der Typ der AWS Resilience Hub Komponente.
   - Quellname — Der Name der Eingabequelle. Wählen Sie einen Quellnamen, um die zugehörigen Details in der jeweiligen Anwendung anzuzeigen. Wenn Sie beispielsweise den Quellnamen wählen, der aus einem AWS CloudFormation Stack importiert wurde, werden Sie auf die Seite mit den Stack-Details auf dem weitergeleitet AWS CloudFormation.
   - Ressourcenanzahl — Die Anzahl der Ressourcen, die der Eingabequelle zugeordnet sind. Wählen Sie eine Zahl, um alle zugehörigen Ressourcen einer Eingabequelle auf der Registerkarte Ressourcen anzuzeigen.
2. Um eine zu erstellen AppComponent, wählen Sie im Menü Aktionen die Option Neu erstellen AppComponent und führen Sie die folgenden Schritte aus:

   a. Geben Sie AppComponent in das Namensfeld einen AppComponentNamen für die ein. Zu Referenzzwecken haben wir dieses Feld vorab mit einem Beispielnamen gefüllt.

   b. Wählen Sie den Typ von AppComponent aus der AppComponentTyp-Dropdown-Liste aus.

c. Wählen Sie Speichern.

3. Um einen zu bearbeiten AppComponent, wählen Sie einen AppComponent aus und wählen Sie dann unter Aktionen die Option Bearbeiten AppComponent aus.
4. Um eine zu löschen AppComponent, wählen Sie eine AppComponent aus und wählen Sie dann AppComponent Aus Aktionen löschen.

Nachdem Sie Änderungen an Ihrer Ressourcenliste vorgenommen haben, erhalten Sie eine Warnung, dass Änderungen an der Entwurfsversion Ihrer Anwendung vorgenommen wurden. Um eine genaue Resilienzbewertung durchführen zu können, müssen Sie eine neue Version Ihrer Anwendung veröffentlichen. Weitere Informationen zum Veröffentlichen einer neuen Version finden Sie unterVeröffentlichung einer neuen AWS Resilience Hub Anwendungsversion.

Verwaltung von Anwendungskomponenten

Eine Anwendungskomponente (AppComponent) ist eine Gruppe verwandter AWS Ressourcen, die als eine Einheit funktionieren und ausfallen. Wenn Sie beispielsweise über eine Primär- und eine Replikatdatenbank verfügen, gehören beide Datenbanken zu derselben AppComponent Datenbank. AWS Resilience Hub hat Regeln, die festlegen, welche AWS Ressourcen zu welchem AppComponent Typ gehören können. Zum Beispiel `DBInstance` kann a zu gehören `AWS::ResilienceHub::DatabaseAppComponent` und nicht zu`AWS::ResilienceHub::ComputeAppComponent`.

Sie AWS Resilience Hub AppComponents unterstützen die folgenden Ressourcen:

- `AWS::ResilienceHub::ComputeAppComponent`
  - `AWS::ApiGateway::RestApi`
  - `AWS::ApiGatewayV2::Api`
  - `AWS::AutoScaling::AutoScalingGroup`
  - `AWS::EC2::Instance`
  - `AWS::ECS::Service`
  - `AWS::EKS::Deployment`
  - `AWS::EKS::ReplicaSet`
  - `AWS::EKS::Pod`
  - `AWS::Lambda::Function`
  - `AWS::StepFunctions::StateMachine`

- `AWS::ResilienceHub::DatabaseAppComponent`
  - `AWS::DocDB::DBCluster`
  - `AWS::DynamoDB::Table`
  - `AWS::RDS::DBCluster`
  - `AWS::RDS::DBInstance`
- `AWS::ResilienceHub::NetworkingAppComponent`
  - `AWS::EC2::NatGateway`
  - `AWS::ElasticLoadBalancing::LoadBalancer`
  - `AWS::ElasticLoadBalancingV2::LoadBalancer`
  - `AWS::Route53::RecordSet`
- `AWS:ResilienceHub::NotificationAppComponent`
  - `AWS::SNS::Topic`
- `AWS::ResilienceHub::QueueAppComponent`
  - `AWS::SQS::Queue`
- `AWS::ResilienceHub::StorageAppComponent`
  - `AWS::Backup::BackupPlan`
  - `AWS::EC2::Volume`
  - `AWS::EFS::FileSystem`
  - `AWS::FSx::FileSystem`

    > **Note**
    >
    > AWS Resilience Hub Unterstützt derzeit nur Amazon FSx for Windows File Server.

  - `AWS::S3::Bucket`

Themen

- Gruppieren von Ressourcen in einer Anwendungskomponente

Gruppieren von Ressourcen in einer Anwendungskomponente

Wenn die Anwendung AWS Resilience Hub zusammen mit ihren Ressourcen importiert wird, AWS Resilience Hub bemüht sich nach besten Kräften, verwandte Ressourcen zu denselben zu

gruppieren AppComponent, was jedoch möglicherweise nicht immer zu 100% korrekt ist. AWS Resilience Hub Führt außerdem die folgenden Aktivitäten aus, nachdem Ihre Anwendung und ihre Ressourcen erfolgreich importiert wurden:

- Scannt Ihre Ressourcen, um zu prüfen, ob sie neu gruppiert werden können AppComponents, um die Genauigkeit der Bewertung zu verbessern.
- Wenn Ressourcen AWS Resilience Hub identifiziert werden, die neu gruppiert werden können AppComponents, werden dieselben als Empfehlungen angezeigt und Sie können diese entweder akzeptieren, ändern (hinzufügen oder entfernen) oder ablehnen. In AWS Resilience Hub gibt das einer Gruppierungsempfehlung zugewiesene Konfidenzniveau den Grad an Sicherheit an, mit dem die Ressourcen anhand ihrer Attribute und Metadaten gruppiert werden sollten. Ein hohes Konfidenzniveau bedeutet, AWS Resilience Hub dass bei einem Konfidenzniveau von 90% oder mehr die Ressourcen in dieser Gruppe miteinander verknüpft sind und gruppiert werden sollten. Ein mittleres Konfidenzniveau bedeutet AWS Resilience Hub bei einem Konfidenzniveau zwischen 70 und 90%, dass die Ressourcen in dieser Gruppe miteinander verknüpft sind und zusammengefasst werden sollten.

> **Note**
>
> AWS Resilience Hub erfordert die richtige Gruppierung, damit die geschätzte Arbeitslast RTO und die geschätzte Arbeitslast berechnet werden können, um Empfehlungen RPO zu generieren.

Im Folgenden finden Sie Beispiele für korrekte Gruppierungen:

- Gruppieren Sie Primärdatenbanken und Replikate in einer einzigen Datenbank. AppComponent
- Gruppieren Sie einen Amazon S3 S3-Bucket und seine Zielreplikation unter einem einzigen AppComponent.
- Gruppieren Sie EC2 Amazon-Instances, die dieselbe Anwendung ausführen, unter einer einzigen AppComponent.
- Gruppieren Sie eine SQS Amazon-Warteschlange und ihre Warteschlange für unzustellbare Briefe zu einer einzigen. AppComponent
- Gruppieren Sie ECS Amazon-Dienste in einer Region und stellen Sie ECS Amazon-Dienste in einer anderen Region als Failover unter einer einzigen AppComponent zusammen.

Weitere Informationen zur Überprüfung und Aufnahme von Empfehlungen zur Gruppierung von AWS Resilience Hub Ressourcen finden Sie in den folgenden Themen:

- AWS Resilience Hub Empfehlungen zur Gruppierung von Ressourcen
- Manuelles Gruppieren von Ressourcen zu einem AppComponent

AWS Resilience Hub Empfehlungen zur Gruppierung von Ressourcen

In diesem Abschnitt wird erklärt, wie Sie Empfehlungen zur Ressourcengruppierung in generieren und überprüfen. AWS Resilience Hub

> **Note**
>
> Mithilfe `AWSResilienceHubAsssessmentExecutionPolicy` AWS verwalteter Richtlinien können Sie die für die Arbeit erforderlichen IAM Berechtigungen erteilen. AWS Resilience Hub Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unterAWSResilienceHubAsssessmentExecutionPolicy.

Um Empfehlungen zur Gruppierung von Ressourcen anzuzeigen

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie Seite „Anwendung hinzufügen“ und dann den Namen der Anwendung aus, für die Sie die Empfehlungen zur Ressourcengruppierung überprüfen möchten.
3. Wählen Sie die Registerkarte Anwendungsstruktur.
4. Wenn eine Informationswarnung AWS Resilience Hub angezeigt wird, wählen Sie Empfehlungen überprüfen, um alle Empfehlungen zur Ressourcengruppierung anzuzeigen. Führen Sie andernfalls die folgenden Schritte aus, um Empfehlungen zur Ressourcengruppierung manuell zu generieren:

   a. Wählen Sie Resources aus.

   b. Wählen Sie im Aktionsmenü die Option Empfehlungen zur Gruppierung abrufen aus.

      AWS Resilience Hub scannt Ihre Ressourcen, um zu überprüfen, wie sie bestmöglich nach Relevanz gruppiert werden können AppComponents , um die Genauigkeit der Bewertungen zu verbessern. Wenn AWS Resilience Hub festgestellt wird, dass Ihre Ressourcen gruppiert werden können, wird eine entsprechende Warnmeldung angezeigt.

c. Wenn die Informationswarnung angezeigt wird, wählen Sie Empfehlungen überprüfen, um alle Empfehlungen zur Ressourcengruppierung anzuzeigen.

Sie können die AppComponents im Abschnitt Empfehlungen zur Ressourcengruppierung überprüfen anhand der folgenden Informationen identifizieren:

- AppComponent Name — Name des Namens, AppComponent in dem die Ressourcen gruppiert werden sollen.
- Konfidenzniveau — Gibt das Konfidenzniveau von AWS Resilience Hub in der Gruppierungsempfehlung an.
- Ressourcenanzahl — Gibt die Anzahl der Ressourcen an, die in der AppComponent gruppiert werden.
- AppComponent Typ — Gibt den Typ von an AppComponent.

Um Ressourcen anzuzeigen, die gruppiert werden AppComponents

1. Führen Sie die im Um Empfehlungen zur Gruppierung von Ressourcen anzuzeigenVerfahren beschriebenen Schritte aus und kehren Sie dann zu diesem Verfahren zurück.
2. Aktivieren Sie im Abschnitt Empfehlungen zur Ressourcengruppierung überprüfen das Kontrollkästchen (neben dem AppComponent Namen), um alle Ressourcen anzuzeigen, die innerhalb der ausgewählten AppComponent Ressourcen gruppiert werden. Wenn Sie mehrere Kontrollkästchen aktivieren, AWS Resilience Hub wird ein dynamisch generierter Abschnitt „Ausgewählte Empfehlungen“ angezeigt, in dem die ausgewählten Empfehlungen AppComponents nach ihrem jeweiligen AppComponent Typ gruppiert werden. Wählen Sie die Zahl unter jedem AppComponent Typ aus, um alle Ressourcen anzuzeigen, die innerhalb des ausgewählten Typs gruppiert werden AppComponent.

   Sie können die Ressourcen, die in den ausgewählten AppComponent Ressourcen gruppiert werden, wie folgt identifizieren:

   - Logische ID — Gibt die logische ID der Ressource an. Eine logische ID ist ein Name, der verwendet wird, um Ressourcen in Ihrem AWS CloudFormation Stack, Ihrer Terraform-Statusdatei, Ihrer manuell hinzugefügten Anwendung, AppRegistry Anwendung oder zu identifizieren. AWS Resource Groups
   - Physikalische ID — Die tatsächlich zugewiesene Kennung für die Ressource, z. B. eine EC2 Amazon-Instance-ID oder ein Amazon S3-Bucket-Name.

- Typ — Gibt den Ressourcentyp an.
- Region — AWS Region, in der sich die Ressource befindet.

Um Empfehlungen zur Gruppierung von Ressourcen zu akzeptieren

1. Führen Sie die im Um Empfehlungen zur Gruppierung von Ressourcen anzuzeigenVerfahren beschriebenen Schritte aus und kehren Sie dann zu diesem Verfahren zurück.
2. Aktivieren Sie im Abschnitt Empfehlungen zur Ressourcengruppierung überprüfen alle Kontrollkästchen neben dem AppComponentNamen. Um nach einem bestimmten Namen zu suchen AppComponent, geben Sie den AppComponent Namen in das AppComponents Feld Suchen ein.

   > **Note**
   >
   > AWS Resilience Hub Zeigt standardmäßig alle Empfehlungen zur Ressourcengruppierung an. Um die Tabelle mit den zuvor abgelehnten Empfehlungen zur Ressourcengruppierung zu filtern, wählen Sie im Dropdownmenü neben dem Feld Suchen die Option Zuvor abgelehnt aus. AppComponents

3. Wählen Sie Accept (Akzeptieren) aus.
4. Wählen Sie im Dialogfeld „Empfehlung zur Ressourcengruppierung akzeptieren“ die Option „Annehmen“.

   AWS Resilience Hub zeigt eine Informationswarnung an, wenn die Ressourcengruppierung erfolgreich war. Wenn Sie nur eine Teilmenge der Empfehlungen zur Ressourcengruppierung akzeptiert haben, werden im Abschnitt Empfehlungen zur Ressourcengruppierung überprüfen alle Empfehlungen zur Ressourcengruppierung angezeigt, die Sie nicht akzeptiert haben.

Um Empfehlungen zur Ressourcengruppierung abzulehnen

1. Führen Sie die im Um Empfehlungen zur Gruppierung von Ressourcen anzuzeigenVerfahren beschriebenen Schritte aus und kehren Sie dann zu diesem Verfahren zurück.
2. Aktivieren Sie im Abschnitt Empfehlungen zur Ressourcengruppierung überprüfen alle Kontrollkästchen neben dem AppComponentNamen. Um nach einem bestimmten Namen zu suchen AppComponent, geben Sie den AppComponent Namen in das AppComponents Feld Suchen ein.

> **Note**
>
> AWS Resilience Hub Zeigt standardmäßig alle Empfehlungen zur Ressourcengruppierung an. Um die Tabelle mit den zuvor abgelehnten Empfehlungen zur Ressourcengruppierung zu filtern, wählen Sie im Dropdownmenü neben dem Feld Suchen die Option Zuvor abgelehnt aus. AppComponents

3. Wählen Sie Reject (Ablehnen).
4. Wählen Sie einen der Gründe für die Ablehnung der Empfehlung zur Ressourcengruppierung aus und wählen Sie dann im Dialogfeld Empfehlung zur Ressourcengruppierung ablehnen die Option Ablehnen aus.

   AWS Resilience Hub zeigt eine Informationswarnung an, die dies bestätigt. Wenn Sie nur eine Teilmenge der Empfehlungen zur Ressourcengruppierung abgelehnt haben, werden im Abschnitt Empfehlungen zur Ressourcengruppierung überprüfen alle Empfehlungen zur Ressourcengruppierung angezeigt, die Sie nicht akzeptiert haben.

Manuelles Gruppieren von Ressourcen zu einem AppComponent

In diesem Abschnitt wird erklärt, wie Sie Ressourcen manuell zu einer gruppieren AppComponent und einer Ressource in verschiedene AppComponent zuweisen. AWS Resilience Hub

Um Ressourcen zu gruppieren

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen den Namen der Anwendung aus, die die Ressourcen enthält, die Sie gruppieren möchten.
3. Wählen Sie die Registerkarte Anwendungsstruktur.
4. Wählen Sie auf der Registerkarte Version die Anwendungsversion mit dem Status Entwurf aus.
5. Wählen Sie die Registerkarte Resources (Ressourcen) aus.
6. Aktivieren Sie die Kontrollkästchen neben Logische ID, um alle Ressourcen auszuwählen, die Sie gruppieren möchten.

> **Note**
>
> Sie können nicht manuell hinzugefügte Ressourcen auswählen.

7. Wählen Sie Aktionen und anschließend Gruppenressourcen aus.
8. Wählen Sie AppComponent aus der AppComponent Dropdownliste Auswählen eine aus, in der Sie die Ressource gruppieren möchten.
9. Wählen Sie Save (Speichern) aus.
10. Wählen Sie Publish new version (Neue Version veröffentlichen) aus.
11. Wählen Sie die Registerkarte Anwendungsstruktur.
12. Gehen Sie wie folgt vor, um die veröffentlichte Version Ihrer Anwendung einzusehen:

    a. Wählen Sie auf der Registerkarte Version die Anwendungsversion mit dem aktuellen Veröffentlichungsstatus aus.

    b. Wählen Sie die Registerkarte Resources (Ressourcen) aus.

Um Ressourcen einem zuzuweisen AppComponent

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen den Namen der Anwendung aus, die die Ressource enthält, die Sie neu gruppieren möchten.
3. Wählen Sie die Registerkarte Anwendungsstruktur.
4. Wählen Sie unter Version die Anwendungsversion mit dem Status Entwurf aus.
5. Wählen Sie die Registerkarte Resources (Ressourcen) aus.
6. Aktivieren Sie das Kontrollkästchen neben Logische ID, um die Ressource auszuwählen.
7. Wählen Sie im AppComponent Menü Aktionen die Option Ändern.
8. Um den aktuellen Namen AppComponent aus dem AppComponentBereich zu löschen, wählen Sie X in der oberen rechten Ecke des Labels, auf dem Ihr aktueller AppComponent Name angezeigt wird.
9. Um die Ressource in einer anderen Gruppe zu gruppieren AppComponent, wählen Sie eine andere Ressource AppComponent aus der AppComponent Dropdownliste „Auswählen“ aus.
10. Wählen Sie Hinzufügen aus.
11. Löschen Sie alle leeren Elemente AppComponents aus dem AppComponentsTab.
12. Wählen Sie Publish new version (Neue Version veröffentlichen) aus.
13. Wählen Sie die Registerkarte Anwendungsstruktur.
14. Gehen Sie wie folgt vor, um die veröffentlichte Version Ihrer Anwendung einzusehen:

a. Wählen Sie auf der Registerkarte Version die Anwendungsversion mit dem aktuellen Veröffentlichungsstatus aus.

b. Wählen Sie die Registerkarte Resources (Ressourcen) aus.

Veröffentlichung einer neuen AWS Resilience Hub Anwendungsversion

Nachdem Sie, wie unter beschrieben, Änderungen an Ihren AWS Resilience Hub Anwendungsressourcen vorgenommen habenAWS Resilience Hub Anwendungsressourcen bearbeiten, müssen Sie eine neue Version Ihrer Anwendung veröffentlichen, um eine genaue Resilienzbewertung durchführen zu können. Außerdem müssen Sie möglicherweise eine neue Version Ihrer Anwendung veröffentlichen, SOPs wenn Sie Ihrer Anwendung neue empfohlene Alarme und Tests hinzugefügt haben.

Um eine neue Version Ihrer Anwendung zu veröffentlichen

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite „Anwendungen“ den Namen der Anwendung aus.
3. Wählen Sie die Registerkarte Anwendungsstruktur.
4. Wählen Sie Publish new version (Neue Version veröffentlichen) aus.
5. Geben Sie im Dialogfeld Version veröffentlichen im Feld Name einen Namen für die Anwendungsversion ein, oder Sie können den von vorgeschlagenen Standardnamen verwenden AWS Resilience Hub.
6. Wählen Sie Publish.

   Wenn Sie eine neue Version Ihrer Anwendung veröffentlichen, wird diese Version bei der Durchführung von Resilienzbewertungen bewertet. Außerdem ist die Entwurfsversion mit der veröffentlichten Version identisch, bis Sie Änderungen vornehmen.

Nachdem Sie eine neue Version Ihrer Anwendung veröffentlicht haben, empfehlen wir Ihnen, einen neuen Resilienzbewertungsbericht zu erstellen, um zu bestätigen, dass Ihre Anwendung weiterhin Ihren Stabilitätsrichtlinien entspricht. Informationen zur Durchführung einer Bewertung finden Sie unter. Durchführung und Verwaltung von AWS Resilience Hub Resilienzbewertungen

Alle Versionen der AWS Resilience Hub Anwendung anzeigen

AWS Resilience Hub Zeigt die Vorgängerversionen Ihrer Anwendung ab dem Zeitpunkt ihrer Erstellung an, damit Sie leichter nachverfolgen können, welche Änderungen an der Anwendung vorgenommen wurden AWS Resilience Hub.

Um alle Versionen Ihrer Anwendung anzuzeigen

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite „Anwendungen“ den Namen der Anwendung aus.
3. Wählen Sie die Registerkarte Anwendungsstruktur.
4. Um alle vorherigen Versionen Ihrer Anwendung anzuzeigen, wählen Sie das Pluszeichen (+) vor Alle Versionen anzeigen. AWS Resilience Hub gibt die Entwurfsversion und die kürzlich veröffentlichte Version Ihrer Anwendung an und gibt jeweils den Status Entwurf und Aktuelle Version an. Sie können eine beliebige Version Ihrer Anwendung auswählen, um deren Ressourcen AppComponent, Eingabequellen und andere zugehörige Informationen anzuzeigen.

   Darüber hinaus können Sie die Liste auch mithilfe einer der folgenden Optionen filtern:

   - Nach Versionsname filtern — Geben Sie einen Namen ein, um die Ergebnisse nach dem Namen Ihrer Anwendungsversion zu filtern.
   - Nach einem Datums- und Zeitbereich filtern — Um diesen Filter anzuwenden, wählen Sie das Kalendersymbol und wählen Sie eine der folgenden Optionen, um nach den Ergebnissen zu filtern, die dem Zeitraum entsprechen:
     - Relativer Bereich — Wählen Sie eine der verfügbaren Optionen aus und klicken Sie auf Anwenden.

       Wenn Sie die Option Benutzerdefinierter Bereich wählen, geben Sie eine Dauer in das Feld Dauer eingeben ein, wählen Sie die entsprechende Zeiteinheit aus der Dropdownliste Zeiteinheit aus und wählen Sie dann Anwenden.
     - Relativer Bereich — Um das Datum und den Zeitraum festzulegen, geben Sie die Start- und Endzeit an und wählen Sie dann Anwenden.

Ressourcen der AWS Resilience Hub Anwendung anzeigen

Um die Ressourcen Ihrer Anwendung anzuzeigen

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen die Anwendung aus, für die Sie die Sicherheitsberechtigungen aktualisieren möchten.
3. Wählen Sie unter Aktionen die Option Ressourcen anzeigen aus.

   Auf der Registerkarte Ressourcen können Sie Ressourcen in der Tabelle Ressourcen wie folgt identifizieren:

   - Logische ID — Eine logische ID ist ein Name, der verwendet wird, um Ressourcen in Ihrem AWS CloudFormation Stack, Ihrer Terraform-Statusdatei, Ihrer manuell hinzugefügten Anwendung, AppRegistry Anwendung oder zu identifizieren. AWS Resource Groups

     > **Note**
     >
     > - Mit Terraform können Sie denselben Namen für verschiedene Ressourcentypen verwenden. Daher sehen Sie am Ende der logischen ID für Ressourcen, die denselben Namen haben, "- Ressourcentyp".
     > - Um die Instanzen aller Anwendungsressourcen anzuzeigen, wählen Sie das Pluszeichen (+) vor der logischen ID. Um alle Instanzen einer Anwendungsressource anzuzeigen, wählen Sie das Pluszeichen (+) vor der logischen ID jeder Ressource.
     >
     > Weitere Informationen zu den unterstützten Ressourcen finden Sie unterthe section called “Unterstützte AWS Resilience Hub Ressourcen”.

   - Status — Gibt an, ob Ihre Ressource auf ihre Resilienz hin bewertet AWS Resilience Hub wird.
   - Ressourcentyp — Der Ressourcentyp identifiziert die Komponentenressource für Ihre Anwendung. `AWS::EC2::Instance`Deklariert beispielsweise eine EC2 Amazon-Instance. Weitere Informationen zum Gruppieren von AppComponent Ressourcen finden Sie unter. Gruppieren von Ressourcen in einer Anwendungskomponente
   - Quellname — Der Name der Eingabequelle. Wählen Sie einen Quellnamen, um die zugehörigen Details in der jeweiligen Anwendung anzuzeigen. Für manuell hinzugefügte Eingabequellen ist der Link nicht verfügbar. Wenn Sie beispielsweise den Quellnamen wählen,

der aus einem AWS CloudFormation Stack importiert wird, werden Sie auf die Seite mit den Stack-Details auf der weitergeleitet AWS CloudFormation.

- Quelltyp — Der Typ der Eingabequelle.
- AppComponent type — Der Typ der Eingangsquelle. Zu den Eingabequellen gehören AWS CloudFormation Stapel, AppRegistry Anwendungen AWS Resource Groups, Terraform-Statusdateien und manuell hinzugefügte Ressourcen.

> **Note**
>
> Um Ihre EKS Amazon-Cluster zu bearbeiten, führen Sie die Schritte unter So bearbeiten Sie die Eingabequellen Ihres AWS Resilience Hub Antragsverfahrens aus.

- Physikalische ID — Die tatsächlich zugewiesene Kennung für diese Ressource, z. B. eine EC2 Amazon-Instance-ID oder ein S3-Bucket-Name.
- Inbegriffen — Dies gibt an, ob AWS Resilience Hub diese Ressourcen in der Anwendung enthalten sind.
- AppComponents— Die AWS Resilience Hub Komponente, die dieser Ressource zugewiesen wurde, als ihre Anwendungsstruktur erkannt wurde.
- Name — Name der Anwendungsressource.
- Konto — Das AWS Konto, dem die physische Ressource gehört.

4. Wählen Sie Speichern und aktualisieren.

Eine AWS Resilience Hub Anwendung löschen

Wenn Sie das Maximum von zehn Anwendungslimits erreicht haben, müssen Sie eine oder mehrere Anwendungen löschen, bevor Sie weitere hinzufügen können.

So löschen Sie eine Anwendung

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen die Anwendung aus, die Sie löschen möchten.
3. Wählen Sie Actions (Aktionen) und anschließend Delete Application (Anwendung löschen).
4. Um den Löschvorgang zu bestätigen, geben Sie im Feld Löschen den Text Löschen ein und wählen Sie Löschen aus.

Konfigurationsparameter der Anwendung

AWS Resilience Hub bietet einen Eingabemechanismus zum Sammeln zusätzlicher Informationen über die Ressourcen, die Ihren Anwendungen zugeordnet sind. Anhand dieser Informationen AWS Resilience Hub erhalten Sie ein tieferes Verständnis Ihrer Ressourcen und können Ihnen bessere Empfehlungen zur Ausfallsicherheit geben.

Im Abschnitt Anwendungskonfigurationsparameter sind alle Konfigurationsparameter für Ihre regionsübergreifende Failover-Unterstützung aufgeführt. AWS Elastic Disaster Recovery Sie können die Konfigurationsparameter wie folgt identifizieren:

- Thema — Gibt den Bereich Ihrer Anwendung an, der konfiguriert ist. Zum Beispiel die Failover-Konfiguration.
- Zweck — Gibt den Grund an, warum die Informationen AWS Resilience Hub angefordert wurden.
- Parameter — Gibt die für den Anwendungsbereich spezifischen Details an, anhand derer Empfehlungen für Ihre Anwendung gegeben AWS Resilience Hub werden. Derzeit verwendet dieser Parameter den Schlüsselwert nur für eine Failover-Region und ein zugeordnetes Konto.

Die Konfigurationsparameter der Anwendung werden aktualisiert

In diesem Abschnitt können Sie die Konfigurationsparameter Ihrer Anwendung aktualisieren AWS Elastic Disaster Recovery und die Anwendung so veröffentlichen, dass sie die aktualisierten Parameter für Resilienzbewertungen enthält.

Um die Konfigurationsparameter der Anwendung zu aktualisieren

1. Wählen Sie im Navigationsbereich Applications (Anwendungen).
2. Wählen Sie auf der Seite Anwendungen den Namen der Anwendung aus, die Sie bearbeiten möchten.
3. Wählen Sie die Registerkarte Anwendungskonfigurationsparameter.
4. Wählen Sie Aktualisieren.
5. Geben Sie die Failover-Konto-ID in das Feld Konto-ID ein.
6. Wählen Sie eine Failover-Region aus der Dropdownliste Region aus.

> **Note**
>
> Wenn Sie diese Funktion deaktivieren möchten, wählen Sie "—" aus der Dropdownliste aus.

7. Wählen Sie „Aktualisieren und veröffentlichen“.

Verwaltung von Resilienzrichtlinien

In diesem Abschnitt wird beschrieben, wie Sie Ausfallsicherheitsrichtlinien für Ihre Anwendungen erstellen. Durch die korrekte Festlegung von Ausfallsicherheitsrichtlinien können Sie sich ein Bild von der Ausfallsicherheit Ihrer Anwendung machen. Eine Ausfallsicherheitsrichtlinie enthält Informationen und Ziele, anhand derer Sie beurteilen können, ob Ihre Anwendung voraussichtlich nach einer Störung, z. B. Software, Hardware, Availability Zone oder Region, wiederhergestellt werden kann. AWS Diese Richtlinien wirken sich nicht auf eine tatsächliche Anwendung aus und wirken sich auch nicht darauf aus. Für mehrere Anwendungen kann dieselbe Ausfallsicherheitsrichtlinie gelten.

Wenn Sie eine Ausfallsicherheitsrichtlinie erstellen, definieren Sie die Zielziele: Recovery Time Objective (RTO) und Recovery Point Objective (RPO). Die Ziele bestimmen, ob die Anwendung die Ausfallsicherheitsrichtlinie erfüllt. Hängen Sie die Richtlinie an Ihre Anwendung an und führen Sie eine Resilienzbewertung durch. Sie können unterschiedliche Richtlinien für die verschiedenen Arten von Anwendungen in Ihrem Portfolio erstellen. Beispielsweise würde eine Echtzeit-Handelsanwendung eine andere Ausfallsicherheitsrichtlinie haben als eine Anwendung mit monatlicher Berichterstattung.

> **Note**
>
> AWS Resilience Hub ermöglicht es Ihnen, den Wert Null in die Felder RTO und RPO Ihrer Resilienz-Richtlinie einzugeben. Bei der Bewertung Ihrer Anwendung liegt das niedrigstmögliche Bewertungsergebnis jedoch nahe Null. Wenn Sie also den Wert Null in die Felder RTO und RPO eingeben, liegen das geschätzte Workload-RTO-Ergebnis und das geschätzte Workload-RPO-Ergebnis nahe Null und der Compliance-Status für Ihre Anwendung wird auf Policy Breached gesetzt.

Bei der Bewertung wird Ihre Anwendungskonfiguration anhand der beigefügten Ausfallsicherheitsrichtlinie bewertet. Am Ende des Prozesses wird bewertet, wie Ihre Anwendung

im Vergleich zu den Wiederherstellungszielen Ihrer AWS Resilience Hub Ausfallsicherheitsrichtlinie abschneidet.

Sie können Resilienzrichtlinien in Anwendungen und auch in Resilienzrichtlinien erstellen. Sie können auf relevante Details zu Ihren Richtlinien zugreifen und diese auch ändern und löschen.

AWS Resilience Hub verwendet Ihre RTO- und RPO-Ziele, um die Widerstandsfähigkeit gegenüber diesen potenziellen Arten von Störungen zu messen:

- Anwendung — Verlust eines erforderlichen Softwaredienstes oder -prozesses.
- Cloud-Infrastruktur — Verlust von Hardware, z. B. EC2-Instanzen.
- Availability Zone (AZ) der Cloud-Infrastruktur — Eine oder mehrere Availability Zones sind nicht verfügbar.
- Cloud-Infrastrukturregion — Eine oder mehrere Regionen sind nicht verfügbar.

AWS Resilience Hub ermöglicht es Ihnen, maßgeschneiderte Ausfallsicherheitsrichtlinien zu erstellen oder unsere empfohlenen, auf offenen Standards basierenden Resilienzrichtlinien zu verwenden. Wenn Sie benutzerdefinierte Richtlinien erstellen, benennen und beschreiben Sie Ihre Richtlinie und wählen Sie die entsprechende Stufe oder Stufe aus, die Ihre Richtlinie definiert. Zu diesen Stufen gehören: grundlegende IT-Kerndienste, geschäftskritisch, kritisch, wichtig und unkritisch.

Wählen Sie die Stufe, die für Ihre Anwendungsklasse geeignet ist. Sie könnten beispielsweise ein Echtzeit-Handelssystem als kritisch einstufen, während Sie eine Anwendung zur monatlichen Berichterstattung als unkritisch einstufen könnten. Wenn Sie unsere Standardrichtlinien verwenden, können Sie eine Ausfallsicherheitsrichtlinie mit einer vorkonfigurierten Stufe und Werten für die RTO- und RPO-Ziele nach Störungsart wählen. Bei Bedarf können Sie die Stufe und die RTO- und RPO-Ziele ändern.

Sie können Resilienzrichtlinien in den Resilienzrichtlinien oder bei der Beschreibung einer neuen Anwendung erstellen.

Resilienzrichtlinien erstellen

In AWS Resilience Hub können Sie eine Resilienzrichtlinie erstellen. Eine Ausfallsicherheitsrichtlinie enthält Informationen und Ziele, anhand derer Sie beurteilen können, ob Ihre Anwendung nach einer Störung wie Software, Hardware, Availability Zone oder AWS Region wieder hergestellt werden kann. Diese Richtlinien wirken sich nicht auf eine tatsächliche Anwendung aus und wirken sich auch nicht darauf aus. Für mehrere Anwendungen kann dieselbe Ausfallsicherheitsrichtlinie gelten.

Wenn Sie eine Resilienzrichtlinie erstellen, definieren Sie die Ziele Recovery Time Objective (RTO) und Recovery Point Objective (RPO). Wenn Sie eine Bewertung durchführen, wird AWS Resilience Hub festgestellt, ob die Anwendung voraussichtlich die in der Resilienz-Richtlinie definierten Ziele erreicht.

Bei der Bewertung wird Ihre Anwendungskonfiguration anhand der beigefügten Ausfallsicherheitsrichtlinie bewertet. Am Ende des Prozesses wird bewertet, AWS Resilience Hub wie Ihre Anwendung im Hinblick auf die Ziele Ihrer Ausfallsicherheitspolitik abschneidet.

> **Note**
>
> AWS Resilience Hub ermöglicht es Ihnen, in die Felder RTO und RPO Ihrer Ausfallsicherheitsrichtlinie den Wert Null einzugeben. Bei der Bewertung Ihrer Anwendung liegt das niedrigstmögliche Bewertungsergebnis jedoch nahe Null. Wenn Sie also den Wert Null in die Felder RTO und RPO eingeben, liegen das geschätzte Workload-RTO-Ergebnis und das geschätzte Workload-RPO-Ergebnis nahe Null und der Compliance-Status für Ihre Anwendung wird auf Policy Breached gesetzt.

Sie können Resilienzrichtlinien in Anwendungen und auch in Resilienzrichtlinien erstellen. Sie können auf relevante Details zu Ihren Richtlinien zugreifen und diese auch ändern und löschen.

Um Resilienzrichtlinien in Anwendungen zu erstellen

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Führen Sie die Verfahren von Anfang bis the section called “Schritt 1: Fügen Sie zunächst eine Anwendung hinzu” Ende durchthe section called “Schritt 8: Fügen Sie Ihrer Anwendung Tags hinzu ”.
3. Wählen Sie im Abschnitt Resilienzrichtlinien die Option Resilienzrichtlinie erstellen aus.

   Die Seite Resilienzrichtlinie erstellen wird angezeigt.
4. Wählen Sie im Abschnitt Erstellungsmethode auswählen die Option Richtlinie erstellen aus.
5. Geben Sie einen Namen für die Richtlinie ein.
6. (Optional) Geben Sie eine Beschreibung für die Richtlinie ein.
7. Wählen Sie aus der Dropdownliste Stufe eine der folgenden Optionen aus:

   - Grundlegende IT-Kerndienste

- Unternehmenskritisch
- Critical
- Wichtig
- Nicht kritisch

8. Geben Sie sowohl für RTO - als auch für RPO-Ziele unter Kundenanwendung RTO und RPO einen numerischen Wert in das Feld ein, und wählen Sie dann die Zeiteinheit aus, für die der Wert steht.

   Wiederholen Sie diese Einträge unter Infrastructure RTO und RPO für Infrastructure and Availability Zone.

9. (Optional) Wenn Sie über eine Anwendung mit mehreren Regionen verfügen, möchten Sie möglicherweise die RTO- und RPO-Ziele einer Region definieren.

   Schalten Sie Region ein. Geben Sie sowohl für Region-RTO als auch für RPO-Ziele unter Kundenanwendung RTO und RPO einen numerischen Wert in das Feld ein, und wählen Sie dann die Zeiteinheit aus, für die der Wert steht.

10. (Optional) Wenn Sie Tags hinzufügen möchten, können Sie dies später tun, während Sie mit der Erstellung Ihrer Richtlinie fortfahren. Weitere Informationen zu Tags finden Sie unter Ressourcen taggen in der AWS allgemeinen Referenz.
11. Um die Richtlinie zu erstellen, wählen Sie Erstellen.

Um Resilienzrichtlinien in Resilienzrichtlinien zu erstellen

1. Wählen Sie im linken Navigationsmenü Richtlinien aus.
2. Wählen Sie im Abschnitt Resilienzrichtlinien die Option Resilienzrichtlinie erstellen aus.

   Die Seite Resilienzrichtlinie erstellen wird angezeigt.

3. Geben Sie einen Namen für die Richtlinie ein.
4. (Optional) Geben Sie eine Beschreibung für die Richtlinie ein.
5. Wählen Sie unter Stufe eine der folgenden Optionen aus:

   - Grundlegende IT-Kerndienste
   - Unternehmenskritisch
   - Critical
   - Wichtig

- Nicht kritisch

6. Geben Sie sowohl für RTO - als auch für RPO-Ziele unter Kundenanwendung RTO und RPO einen numerischen Wert in das Feld ein und wählen Sie dann die Zeiteinheit aus, für die der Wert steht.

   Wiederholen Sie diese Einträge unter Infrastructure RTO und RPO für Infrastructure and Availability Zone.

7. (Optional) Wenn Sie über eine Anwendung mit mehreren Regionen verfügen, möchten Sie möglicherweise die RTO- und RPO-Ziele einer Region definieren.

   Schalten Sie Region ein. Geben Sie sowohl für RTO - als auch für RPO-Ziele unter Kundenanwendung RTO und RPO einen numerischen Wert in das Feld ein und wählen Sie dann die Zeiteinheit aus, für die der Wert steht.

8. (Optional) Wenn Sie Tags hinzufügen möchten, können Sie dies später tun, während Sie mit der Erstellung Ihrer Richtlinie fortfahren. Weitere Informationen zu Tags finden Sie unter Ressourcen taggen in der AWS allgemeinen Referenz.
9. Um die Richtlinie zu erstellen, wählen Sie Erstellen.

Um Resilienzrichtlinien auf der Grundlage einer vorgeschlagenen Richtlinie zu erstellen

1. Wählen Sie im linken Navigationsmenü Richtlinien aus.
2. Wählen Sie im Abschnitt Wählen Sie eine Erstellungsmethode aus die Option Wählen Sie eine Richtlinie aus, die auf einer vorgeschlagenen Richtlinie basiert.
3. Wählen Sie im Abschnitt Resilienzrichtlinien die Option Resilienzrichtlinie erstellen aus.

   Die Seite Resilienzrichtlinie erstellen wird angezeigt.

4. Geben Sie einen Namen für die Resilienzrichtlinie ein.
5. (Optional) Geben Sie eine Beschreibung für die Richtlinie ein.
6. Sehen Sie sich im Abschnitt Vorgeschlagene Resilienzrichtlinien eine der folgenden vordefinierten Stufen der Stabilitätsrichtlinien an und wählen Sie sie aus:

   - Nicht kritische Anwendung
   - Wichtiger Antrag
   - Kritische Anwendung
   - Globale kritische Anwendung

- Geschäftskritische Anwendung
- Weltweite unternehmenskritische Anwendung
- Grundlegender Kernservice

7. Um die Resilienzrichtlinie zu erstellen, wählen Sie Create policy aus.

Zugreifen auf Details zur Resilienzrichtlinie

Wenn Sie eine Resilienzrichtlinie öffnen, werden Ihnen wichtige Details zu der Richtlinie angezeigt. Sie können die Resilienz auch bearbeiten oder löschen.

Die Details zur Ausfallsicherheitsrichtlinie bestehen aus zwei Hauptansichten: Zusammenfassung und Tags.

Übersicht

Grundlegende Informationen

Stellt die folgenden Informationen zur Ausfallsicherheitsrichtlinie bereit: Name, Beschreibung, Stufe, Kostenstufe und Erstellungsdatum.

Geschätztes Workload-RTO und geschätztes Workload-RPO

Zeigt den geschätzten Workload-RTO und den geschätzten Workload-RPO-Störungstyp an, die mit dieser Ausfallsicherheitsrichtlinie verknüpft sind.

Tags

Verwenden Sie diese Ansicht, um anwendungsinterne Tags zu verwalten, hinzuzufügen und zu löschen.

Um Resilienzrichtlinien in den Resilienzrichtlinien-Details zu bearbeiten

1. Wählen Sie im linken Navigationsmenü Richtlinien aus.
2. Öffnen Sie unter Resilienzrichtlinien eine Resilienzrichtlinie.
3. Wählen Sie Bearbeiten aus. Geben Sie die entsprechenden Änderungen in den Feldern Basisinformationen sowie RTO und RPO ein. Wählen Sie dann Save changes (Änderungen speichern).

Um Resilienzrichtlinien in der Resilienzrichtlinie zu bearbeiten

1. Wählen Sie im linken Navigationsmenü Richtlinien aus.
2. Wählen Sie unter Resilienzrichtlinien eine Resilienzrichtlinie aus.
3. Wählen Sie Aktionen und dann Bearbeiten aus.
4. Geben Sie die entsprechenden Änderungen in den Feldern Basisinformationen sowie RTO und RPO ein. Wählen Sie dann Save changes (Änderungen speichern).

Um Resilienzrichtlinien in den Resilienzrichtlinien-Details zu löschen

1. Wählen Sie im linken Navigationsmenü Richtlinien aus.
2. Öffnen Sie unter Resilienzrichtlinien eine Resilienzrichtlinie.
3. Wählen Sie Löschen aus. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen aus.

Um Resilienzrichtlinien in der Resilienzrichtlinie zu löschen

1. Wählen Sie im linken Navigationsmenü Richtlinien aus.
2. Wählen Sie unter Resilienzrichtlinien eine Resilienzrichtlinie aus.
3. Wählen Sie Aktionen und dann Löschen aus.
4. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Durchführung und Verwaltung von AWS Resilience Hub Resilienzbewertungen

Wenn sich Ihre Anwendung ändert, sollten Sie eine Resilienzbewertung durchführen. Bei der Bewertung wird jede Konfiguration der Anwendungskomponente mit der Richtlinie verglichen und es werden Alarm- SOP und Testempfehlungen ausgesprochen. Diese Konfigurationsempfehlungen können die Geschwindigkeit der Wiederherstellungsverfahren verbessern.

Alarmempfehlungen helfen Ihnen bei der Einrichtung von Alarmen, die Ausfälle erkennen. SOPIn den Empfehlungen stehen Skripts zur Verfügung, die allgemeine Wiederherstellungsprozesse verwalten, z. B. die Wiederherstellung aus einem Backup. Die Testempfehlungen enthalten Vorschläge, mit denen Sie überprüfen können, ob Ihre Konfigurationen ordnungsgemäß funktionieren. Sie können beispielsweise testen, ob eine Anwendung bei automatischen Wiederherstellungsprozessen wie automatischer Skalierung oder Lastenausgleich aufgrund von Netzwerkproblemen wiederhergestellt

wird. Sie können testen, ob Anwendungsalarme ausgelöst werden, wenn Ressourcen ihre Grenzen erreichen. Sie können auch testen, wie gut es unter den von Ihnen angegebenen Bedingungen SOPs funktioniert.

Durchführung von Resilienzbewertungen

Sie können einen Bericht zur Resilienzbewertung von mehreren Standorten in ausführen. AWS Resilience Hub Weitere Informationen zu Ihrer Anwendung finden Sie unterthe section called “Verwalten von Anwendungen”.

So führen Sie eine Resilienzbewertung über das Menü Aktionen aus

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Wählen Sie eine Anwendung aus der Tabelle Anwendungen aus.
3. Wählen Sie im Menü Aktionen die Option Resilienz bewerten.
4. Im Dialogfeld Resilienzbewertung ausführen können Sie einen eindeutigen Namen eingeben oder den generierten Namen für die Bewertung verwenden.
5. Wählen Sie Ausführen aus.

   Um den Bewertungsbericht zu überprüfen, wählen Sie in Ihrer Anwendung Assessments aus. Weitere Informationen finden Sie unter the section called “Überprüfung der Bewertungsberichte”.

Um eine Resilienzbewertung auf der Registerkarte Bewertungen durchzuführen

Sie können eine neue Resilienzbewertung durchführen, wenn sich Ihre Anwendung oder Resilienzrichtlinie ändert.

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Wählen Sie eine Anwendung aus der Tabelle Anwendungen aus.
3. Wählen Sie die Registerkarte „Assessments“.
4. Wählen Sie Resilienzbewertung ausführen aus.
5. Im Dialogfeld Resilienzbewertung ausführen können Sie einen eindeutigen Namen eingeben oder den generierten Namen für die Bewertung verwenden.
6. Wählen Sie Ausführen aus.

   Um den Bewertungsbericht zu überprüfen, wählen Sie in Ihrer Anwendung Assessments aus. Weitere Informationen finden Sie unter the section called “Überprüfung der Bewertungsberichte”.

Überprüfung der Bewertungsberichte

Bewertungsberichte finden Sie in der Ansicht „Assessments“ Ihrer Anwendung.

Um einen Bewertungsbericht zu finden

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Öffnen Sie unter Anwendungen eine Anwendung.
3. Wählen Sie auf der Registerkarte Bewertungen einen Bewertungsbericht aus der Tabelle Resilienzbewertungen aus.

Wenn Sie den Bericht öffnen, sehen Sie Folgendes:

- Ein Gesamtüberblick über den Bewertungsbericht
- Empfehlungen zur Verbesserung der Resilienz.
- Empfehlungen zur Einrichtung von Alarmen SOPs und Tests
- Wie erstelle und verwalte ich Tags, um deine AWS Ressourcen zu durchsuchen und zu filtern

Prüfen

Dieser Abschnitt bietet einen Überblick über den Bewertungsbericht. AWS Resilience Hub listet jeden Störungstyp und die zugehörige Anwendungskomponente auf. Außerdem werden Ihre aktuellen Richtlinien RTO und Ihre RPO Richtlinien aufgeführt und es wird festgestellt, ob die Anwendungskomponente die Richtlinienziele erreichen kann.

Übersicht

Zeigt den Namen der Anwendung, den Namen der Resilienzrichtlinie und das Erstellungsdatum des Berichts an.

Es wurden Ressourcenverschiebungen festgestellt

In diesem Abschnitt werden alle Ressourcen aufgeführt, die hinzugefügt oder entfernt wurden, nachdem sie in die neueste Version der veröffentlichten Anwendung aufgenommen wurden. Wählen Sie Eingabequellen erneut importieren, um alle Eingabequellen (die Ressourcen enthalten) auf der Registerkarte Eingabequellen erneut zu importieren. Wählen Sie „Veröffentlichen und bewerten“, um die aktualisierten Ressourcen in die Anwendung aufzunehmen und eine genaue Bewertung der Belastbarkeit zu erhalten.

Sie können die fehlerhaften Eingabequellen anhand der folgenden Methoden identifizieren:

- Logische ID — Gibt die logische ID der Ressource an. Eine logische ID ist ein Name, der verwendet wird, um Ressourcen in Ihrem AWS CloudFormation Stack, Ihrer Terraform-Statusdatei, Ihrer manuell hinzugefügten Anwendung, AppRegistry Anwendung oder zu identifizieren. AWS Resource Groups
- Änderung — Gibt an, ob eine Eingaberessource hinzugefügt oder entfernt wurde.
- Quellname — Gibt den Namen der Ressource an. Wählen Sie einen Quellnamen, um die zugehörigen Details in der jeweiligen Anwendung anzuzeigen. Für manuell hinzugefügte Eingabequellen ist der Link nicht verfügbar. Wenn Sie beispielsweise den Quellnamen wählen, der aus einem AWS CloudFormation Stack importiert wird, werden Sie auf die Seite mit den Stack-Details auf der weitergeleitet AWS CloudFormation.
- Ressourcentyp — Gibt den Ressourcentyp an.
- Konto — Gibt das AWS Konto an, dem die physische Ressource gehört.
- Region — Gibt die AWS Region an, in der sich die Ressource befindet.

RTO

Zeigt grafisch an, ob die Anwendung voraussichtlich die Ziele der Stabilitätsrichtlinie erfüllt. Dies basiert auf der Zeitspanne, in der eine Anwendung ausgefallen sein kann, ohne dass das Unternehmen nennenswert geschädigt wird. Die Bewertung gibt einen geschätzten Arbeitsaufwand anRTO.

RPO

Zeigt in grafischer Darstellung, ob die Anwendung voraussichtlich die Ziele der Stabilitätsrichtlinie erfüllt. Dies basiert auf der Zeitspanne, in der Daten verloren gehen können, bevor ein erheblicher Schaden für das Unternehmen eintritt. Die Bewertung gibt einen geschätzten Arbeitsaufwand anRPO.

Details

In den Registerkarten Alle Ergebnisse und Abweichungen bei der Anwendungskonformität werden die einzelnen Störungstypen detailliert beschrieben. Auf der Registerkarte „Alle Ergebnisse“ werden alle Störungen einschließlich Abweichungen bei der Einhaltung von Vorschriften angezeigt, und auf der Registerkarte „Abweichungen bei der Anwendungskonformität“ werden nur Abweichungen bei der Einhaltung der Vorschriften angezeigt. Die Art der Störung umfasst Anwendung, Cloud-Infrastruktur (Infrastruktur und Availability Zone) und Region und bietet die folgenden Informationen dazu:

- AppComponent

  Die Ressourcen, aus denen die Anwendung besteht. Ihre Anwendung könnte beispielsweise eine Datenbank- oder Rechenkomponente haben.

- Geschätzt RTO

  Gibt an, ob Ihre Richtlinienkonfiguration Ihren Richtlinienanforderungen entspricht. Wir geben zwei Werte an: unseren geschätzten Wert RTO und Ihren RTOZielwert. Wenn Sie beispielsweise unter Zielwert einen Wert von 2 Stunden RTO und unter „Geschätzter Arbeitsaufwand“ einen Wert von 40 Minuten sehenRTO, bedeutet dies, dass wir einen geschätzten Arbeitsaufwand RTO von 40 Minuten angeben, während RTO der aktuelle Arbeitsaufwand für Ihre Bewerbung bei zwei Stunden liegt. Wir stützen unsere geschätzte Arbeitsauslastung RTO auf die Konfiguration, nicht auf die Richtlinie. Daher hat eine Multi-Availability Zone-Datenbank bei einem Ausfall der Availability Zone dieselbe geschätzte ArbeitslastRTO, unabhängig davon, welche Richtlinie Sie wählen.

- RTODrift

  Gibt die Dauer an, um die Ihre Bewerbung von der geschätzten Arbeitslast RTO der vorherigen erfolgreichen Prüfung abgewichen ist. Wir geben zwei Werte an: „Geschätzt“ RTO und „RTODrift“. Wenn Sie beispielsweise den Wert 2 Stunden unter Geschätzt RTO und 40 m unter RTOAbweichung sehen, bedeutet dies, dass Ihre Anwendung um 40 Minuten von der geschätzten Arbeitslast RTO der vorherigen erfolgreichen Bewertung abweicht.

- Geschätzt RPO

  Zeigt die tatsächliche RPO Richtlinie „Geschätzte Arbeitslast“ an, die auf der Grundlage der RPOZielrichtlinie geschätzt wird, die Sie für jede Anwendungskomponente festgelegt haben. AWS Resilience Hub Möglicherweise haben Sie in Ihrer Ausfallsicherheitsrichtlinie das RPO Ziel für Ausfälle in der Availability Zone auf eine Stunde festgelegt. Das geschätzte Ergebnis könnte nahe Null berechnet werden. Dies setzt voraus, dass Amazon Aurora, wo wir jede Transaktion festschreiben, in vier von sechs Knoten, die sich über mehrere Availability Zones erstrecken, erfolgreich ist. Die point-in-time Wiederherstellung kann fünf Minuten dauern.

  Das einzige RTO RPO Ziel, das Sie nicht beliefern können, ist die Region. Bei einigen Anwendungen ist es sinnvoll, die Wiederherstellung zu planen, wenn eine wichtige Abhängigkeit von einem AWS Dienst besteht, der möglicherweise in der gesamten Region nicht mehr verfügbar ist.

Wenn Sie sich für diese Option entscheiden, z. B. die Festlegung RTO von RPO Zielen für die Region, erhalten Sie eine geschätzte Wiederherstellungszeit und Betriebsempfehlungen für solche Ausfälle.

- RPODrift

  Gibt die Dauer an, um die Ihre Bewerbung von der geschätzten Arbeitslast RPO der vorherigen erfolgreichen Prüfung abgewichen ist. Wir geben zwei Werte an: „Geschätzt“ RPO und „RPODrift“. Wenn Sie beispielsweise den Wert 2 Stunden unter Geschätzt RPO und 40 m unter RPOAbweichung sehen, bedeutet dies, dass Ihre Anwendung um 40 Minuten von der geschätzten Arbeitslast RPO der vorherigen erfolgreichen Bewertung abweicht.

Überprüfung der Empfehlungen zur Ausfallsicherheit

In den Empfehlungen zur Resilienz werden die Anwendungskomponenten bewertet und Empfehlungen zur Optimierung anhand der geschätzten Arbeitslast RTO und der geschätzten ArbeitslastRPO, der Kosten und der minimalen Änderungen gegeben.

Mit AWS Resilience Hub können Sie die Ausfallsicherheit mithilfe einer der folgenden empfohlenen Optionen optimieren, die im Abschnitt Warum Sie diese Option wählen sollten:

> **Note**
>
> - AWS Resilience Hub bietet bis zu drei AWS Resilience Hub empfohlene Optionen.
> - Wenn Sie „Region“ RTO und „RPOZiele“ festlegen, AWS Resilience Hub wird RPO in den empfohlenen Optionen „Für Region optimieren“RTO/angezeigt. Wenn Regional RTO und RPO Targets nicht festgelegt sind, RPO wird Optimize for Availability Zone (AZ)RTO/angezeigt. Weitere Informationen zum Festlegen von regionalen RTO RPO /-Zielen bei der Erstellung von Ausfallsicherheitsrichtlinien finden Sie unterResilienzrichtlinien erstellen .
> - Die geschätzte Arbeitslast RTO und die geschätzten RPO Arbeitslastwerte für die Anwendungen und ihre Konfigurationen werden unter Berücksichtigung der Datenmenge und der einzelnen AppComponents Benutzer bestimmt. Bei diesen Werten handelt es sich jedoch nur um Schätzungen. Sie sollten Ihre eigenen Tests (z. B. Amazon Fault Injection Service) verwenden, um Ihre Anwendung auf tatsächliche Wiederherstellungszeiten zu testen.

Für die Availability Zone optimierenRTO/RPO

Die niedrigstmögliche geschätzte Wiederherstellungszeit (RTO/RPO) für Workloads während einer Unterbrechung der Availability Zone (AZ). Wenn Ihre Konfiguration nicht ausreichend geändert werden kann, um die RPO Ziele RTO und zu erreichen, werden Sie über die niedrigsten geschätzten Wiederherstellungszeiten für Workload AZ informiert, damit Ihre Konfiguration der Möglichkeit nahe kommt, die Richtlinie einzuhalten.

Für Region optimierenRTO/RPO

Die niedrigstmögliche geschätzte Wiederherstellungszeit (RTO/RPO) für Workloads während einer regionalen Störung. Wenn Ihre Konfiguration nicht ausreichend geändert werden kann, um die RPO Ziele von RTO und zu erreichen, werden Sie über die Wiederherstellungszeiten in der Region mit der niedrigsten geschätzten Auslastung informiert, damit Ihre Konfiguration der Möglichkeit nahe kommt, die Richtlinie einzuhalten.

Optimieren Sie im Hinblick auf die Kosten

Die niedrigsten Kosten, die Ihnen bei gleichzeitiger Einhaltung Ihrer Ausfallsicherheitsrichtlinien entstehen können. Wenn Ihre Konfiguration nicht ausreichend geändert werden kann, um die Optimierungsziele zu erreichen, werden Sie über die niedrigsten Kosten informiert, die Ihnen entstehen können, um Ihre Konfiguration so weit wie möglich zu bringen, die Richtlinie einzuhalten.

Optimieren Sie für minimale Änderungen

Die minimalen Änderungen, die erforderlich sind, um Ihre politischen Ziele zu erreichen. Wenn Ihre Konfiguration nicht ausreichend geändert werden kann, um die Optimierungsziele zu erreichen, werden Sie über die empfohlenen Änderungen informiert, mit denen Ihre Konfiguration der Möglichkeit, die Richtlinie zu erfüllen, sehr nahe kommen kann.

Die folgenden Elemente sind in den Aufschlüsselungen nach Optimierungskategorien enthalten:

- Beschreibung

  Beschreibt die von AWS Resilience Hub vorgeschlagenen Konfigurationen.
- Änderungen

  Eine Liste von Textänderungen, in denen die Aufgaben beschrieben werden, die erforderlich sind, um zur vorgeschlagenen Konfiguration zu wechseln.
- Grundkosten

Die geschätzten Kosten im Zusammenhang mit den empfohlenen Änderungen.

> **Note**
>
> Die Grundkosten können je nach Nutzung variieren und beinhalten keine Rabatte oder Angebote aus dem Enterprise-Rabattprogramm (EDP).

- Geschätzter Arbeitsaufwand RTO und RPO

  Der geschätzte Arbeitsaufwand RTO und der geschätzte Arbeitsaufwand RPO nach Änderungen.

AWSResilience Hub bewertet, ob eine Anwendungskomponente (AppComponent) eine Ausfallsicherheitsrichtlinie einhalten kann. Wenn der einer Resilienzrichtlinie AppComponent nicht entspricht und AWS Resilience Hub keine Empfehlungen aussprechen kann, um die Einhaltung zu erleichtern, kann dies daran liegen, dass die Wiederherstellungszeit für die ausgewählte Komponente AppComponent nicht innerhalb der Einschränkungen von eingehalten werden kann. AppComponent Zu den AppComponent Einschränkungen gehören beispielsweise Ressourcentyp, Speichergröße oder Ressourcenkonfiguration.

Um die AppComponent Einhaltung der Resilienz-Richtlinie zu erleichtern, ändern Sie den Ressourcentyp der AppComponent oder aktualisieren Sie die Resilienz-Richtlinie, um sie an das anzupassen, was die Ressource bieten kann.

Überprüfung der operativen Empfehlungen

Betriebsempfehlungen enthalten Empfehlungen zur Einrichtung von Alarmen und AWS FIS Experimenten anhand von AWS CloudFormation Vorlagen. SOPs

AWS Resilience Hub stellt AWS CloudFormation Vorlagendateien bereit, mit denen Sie die Infrastruktur der Anwendung als Code herunterladen und verwalten können. Aus diesem Grund stellen wir Empfehlungen bereit, AWS CloudFormation damit Sie sie Ihrem Anwendungscode hinzufügen können. Wenn die Größe der AWS CloudFormation Vorlagendatei mehr als ein MB beträgt und mehr als 500 Ressourcen enthält, AWS Resilience Hub generiert sie mehr als eine AWS CloudFormation Vorlagendatei, wobei die Größe jeder Datei nicht mehr als ein MB beträgt und bis zu 500 Ressourcen enthält. Wenn die AWS CloudFormation Vorlagendatei in mehrere Dateien aufgeteilt ist, werden die Namen der AWS CloudFormation Vorlagendateien mit angehängt`partXofY`, wobei `X` die Dateinummer in der Reihenfolge und die Gesamtzahl der Dateien `Y` angegeben wird, in die die AWS CloudFormation Vorlagendatei aufgeteilt ist. Wenn die Vorlagendatei beispielsweise in vier

Dateien aufgeteilt `big-app-template5-Alarm-104849185070-us-west-2.yaml` ist, lauten die Dateinamen wie folgt:

- `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`

Bei großen AWS CloudFormation Vorlagen werden Sie jedoch aufgefordert, den Amazon Simple Storage Service bereitzustellen, URI anstattCLI/APImit der lokalen Datei als Eingabe zu verwenden.

AWS Resilience Hub In können Sie die folgenden Aktionen ausführen:

- Sie können die ausgewählten Alarme SOPs und AWS FIS Experimente bereitstellen. Um Alarme und AWS FIS Experimente bereitzustellenSOPs, wählen Sie die entsprechende Empfehlung aus und geben Sie einen eindeutigen Namen ein. AWS Resilience Hub erstellt eine Vorlage auf der Grundlage Ihrer ausgewählten Empfehlungen. Unter Vorlagen können Sie über einen Amazon Simple Storage Service (Amazon S3) auf Ihre erstellten Vorlagen zugreifenURL.
- Sie können ausgewählte Alarme und AWS FIS ExperimenteSOPs, die zu einem beliebigen Zeitpunkt für Ihre Anwendung empfohlen wurden, ein- oder ausschließen. Weitere Informationen finden Sie unter the section called “Einschließlich oder ohne betriebliche Empfehlungen”.
- Sie können auch nach einer Anwendung nach Tags suchen, sie erstellen, hinzufügen, entfernen und verwalten und alle damit verknüpften Tags anzeigen.

Einschließlich oder ohne betriebliche Empfehlungen

AWS Resilience Hub bietet eine Option zum Ein- oder Ausschließen der Alarme und AWS FIS Experimente (Tests), die zur Verbesserung der Ausfallsicherheit Ihrer Anwendung zu einem beliebigen Zeitpunkt empfohlen wurden. SOPs Das Ein- und Ausschließen betrieblicher Empfehlungen wirkt sich erst dann auf den Stabilitätswert Ihrer Anwendung aus, wenn Sie eine neue Bewertung durchführen. Daher empfehlen wir Ihnen, eine Bewertung durchzuführen, um den aktualisierten Resilienz-Score zu erhalten und zu verstehen, wie sich dieser auf Ihre Anwendung auswirkt.

Weitere Informationen zur Einschränkung der Berechtigungen zum Einschließen oder Ausschließen von Empfehlungen pro Anwendung finden Sie unter. the section called “Einschränkung der Berechtigungen zum Ein- oder Ausschließen von AWS Resilience Hub Empfehlungen”

So schließen Sie Betriebsempfehlungen in Anwendungen ein oder aus

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Öffnen Sie unter Anwendungen eine Anwendung.
3. Wählen Sie Assessments und wählen Sie eine Bewertung aus der Tabelle Resiliency Assessments aus. Wenn Sie noch keine Bewertung haben, schließen Sie das Verfahren unter ab the section called “Durchführung von Resilienzbewertungen” und kehren Sie dann zu diesem Schritt zurück.
4. Wählen Sie die Registerkarte Betriebsempfehlungen aus.
5. Gehen Sie wie folgt vor, um betriebliche Empfehlungen in Ihren Antrag aufzunehmen oder daraus auszuschließen:

Um empfohlene Alarme in Ihre Anwendung aufzunehmen oder auszuschließen

1. Gehen Sie wie folgt vor, um Alarme auszuschließen:
   a. Wählen Sie auf der Registerkarte Alarme in der Tabelle Alarme alle Alarme (mit dem Status Nicht implementiert) aus, die Sie ausschließen möchten. Den aktuellen Implementierungsstatus eines Alarms können Sie der Spalte Status entnehmen.
   b. Wählen Sie unter Aktionen die Option Ausgewählte ausschließen aus.
   c. Wählen Sie im Dialogfeld „Empfehlungen ausschließen“ einen der folgenden Gründe aus (optional) und wählen Sie Ausgewählte ausschließen aus, um die ausgewählten Alarme aus der Anwendung auszuschließen.
      - Bereits implementiert — Wählen Sie diese Option, wenn Sie diese Alarme bereits in einem AWS Service wie Amazon CloudWatch oder einem anderen Drittanbieter implementiert haben.
      - Nicht relevant — Wählen Sie diese Option, wenn die Alarme nicht Ihren Geschäftsanforderungen entsprechen.
      - Zu kompliziert in der Implementierung — Wählen Sie diese Option, wenn Sie der Meinung sind, dass die Implementierung dieser Alarme zu kompliziert ist.
      - Andere — Wählen Sie diese Option, um einen anderen Grund für den Ausschluss der Empfehlung anzugeben.
2. Gehen Sie wie folgt vor, um Alarme einzubeziehen:

a. Wählen Sie auf der Registerkarte Alarme in der Tabelle Alarme alle Alarme (mit dem Status Ausgeschlossen) aus, die Sie einbeziehen möchten. Den aktuellen Implementierungsstatus des Alarms können Sie der Spalte Status entnehmen.

b. Wählen Sie unter Aktionen die Option Ausgewählte einbeziehen aus.

c. Wählen Sie im Dialogfeld „Empfehlungen einbeziehen“ die Option Ausgewählte einbeziehen, um alle ausgewählten Alarme in Ihre Anwendung aufzunehmen.

Um empfohlene Standardarbeitsanweisungen (SOPs) in Ihre Anwendung aufzunehmen oder daraus auszuschließen

1. Gehen Sie wie folgt vorSOPs, um empfohlene Empfehlungen auszuschließen:

   a. Wählen Sie auf der Registerkarte Standardarbeitsanweisungen aus der SOPsTabelle alle SOPs (mit dem Status Implementiert oder Nicht implementiert) aus, die Sie ausschließen möchten. Sie können den aktuellen Implementierungsstatus eines SOP anhand der Spalte Status ermitteln.

   b. Wählen Sie unter Aktionen die Option Ausgewählte ausschließen aus, um die ausgewählten Personen SOPs aus Ihrer Anwendung auszuschließen.

   c. Wählen Sie im Dialogfeld „Empfehlungen ausschließen“ einen der folgenden Gründe aus (optional) und wählen Sie Ausgewählte ausschließen, um die ausgewählten Personen SOPs aus der Anwendung auszuschließen.

      - Bereits implementiert — Wählen Sie diese Option, wenn Sie diese bereits SOPs in einem AWS Service oder einem anderen Drittanbieter implementiert haben.
      - Nicht relevant — Wählen Sie diese Option, wenn SOPs sie nicht Ihren Geschäftsanforderungen entspricht.
      - Zu kompliziert zu implementieren — Wählen Sie diese Option, wenn Sie der Meinung SOPs sind, dass die Implementierung zu kompliziert ist.
      - Keine — Wählen Sie diese Option, wenn Sie den Grund nicht angeben möchten.

2. Führen Sie zum SOPs Einschließen die folgenden Schritte aus:

   a. Wählen Sie auf der Registerkarte Standardarbeitsanweisungen aus der SOPsTabelle alle Alarme (mit dem Status Ausgeschlossen) aus, die Sie einbeziehen möchten. Den aktuellen Implementierungsstatus des Alarms können Sie der Spalte Status entnehmen.

   b. Wählen Sie unter Aktionen die Option Ausgewählte einbeziehen aus.

c. Wählen Sie im Dialogfeld „Empfehlungen einbeziehen“ die Option Ausgewählte einbeziehen, um alle SOPs in Ihrer Anwendung ausgewählten Elemente einzubeziehen.

Um empfohlene Tests in Ihre Anwendung aufzunehmen oder auszuschließen

1. Gehen Sie wie folgt vor, um empfohlene Tests auszuschließen:

   a. Wählen Sie auf der Registerkarte Vorlagen für Fault-Injection-Experimente in der Tabelle mit den Versuchsvorlagen für Fehlerinjektionen alle Tests (mit dem Status Implementiert oder Nicht implementiert) aus, die Sie ausschließen möchten. Den aktuellen Implementierungsstatus eines Tests können Sie der Spalte Status entnehmen.

   b. Wählen Sie unter Aktionen die Option Ausgewählte ausschließen aus.

   c. Wählen Sie im Dialogfeld „Empfehlungen ausschließen“ einen der folgenden Gründe aus (optional) und wählen Sie Ausgewählte ausschließen aus, um die ausgewählten AWS FIS Experimente aus der Anwendung auszuschließen.

      - Bereits implementiert — Wählen Sie diese Option, wenn Sie diese Tests bereits in einem AWS Dienst oder einem anderen Drittanbieter implementiert haben.
      - Nicht relevant — Wählen Sie diese Option, wenn die Tests nicht Ihren Geschäftsanforderungen entsprechen.
      - Zu kompliziert zu implementieren — Wählen Sie diese Option, wenn Sie der Meinung sind, dass die Implementierung dieser Tests zu kompliziert ist.
      - Keine — Wählen Sie diese Option, wenn Sie den Grund nicht angeben möchten.

2. Gehen Sie wie folgt vor, um empfohlene Tests einzubeziehen:

   a. Wählen Sie auf der Registerkarte Vorlagen für Experimente mit Fehlerinjektion in der Tabelle mit Versuchsvorlagen für Fehlerinjektionen alle Tests (mit dem Status Ausgeschlossen) aus, die Sie einbeziehen möchten. Den aktuellen Implementierungsstatus des Tests können Sie der Spalte Status entnehmen.

   b. Wählen Sie unter Aktionen die Option Ausgewählte einbeziehen aus.

   c. Wählen Sie im Dialogfeld Empfehlungen einbeziehen die Option Ausgewählte einbeziehen aus, um alle ausgewählten Tests in Ihre Anwendung aufzunehmen.

Resilienzbewertungen löschen

Sie können Resilienzbewertungen in der Bewertungsansicht Ihrer Anwendung löschen.

Um eine Resilienzbewertung zu löschen

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Öffnen Sie unter Anwendungen eine Anwendung.
3. Wählen Sie unter Assessments in der Tabelle Resiliency Assessments einen Bewertungsbericht aus.
4. Um die Löschung zu bestätigen, klicken Sie auf Delete (Löschen).

   Der Bericht wird nicht mehr in der Tabelle Resilienzbewertungen angezeigt.

Verwalten von Alarmen

Wenn Sie eine Resilienzbewertung durchführen, AWS Resilience Hub empfiehlt es sich im Rahmen der Betriebsempfehlungen, CloudWatch Amazon-Alarme einzurichten, um die Ausfallsicherheit Ihrer Anwendungen zu überwachen. Wir empfehlen diese Alarme auf der Grundlage der Ressourcen und Komponenten Ihrer aktuellen Anwendungskonfiguration. Wenn sich die Ressourcen und Komponenten in Ihrer Anwendung ändern, sollten Sie eine Resilienzbewertung durchführen, um sicherzustellen, dass Sie über die richtigen Alarme für Ihre aktualisierte Anwendung verfügen.

AWS Resilience Hub stellt eine Vorlagendatei (`README.md`) bereit, mit der Sie Alarme erstellen können, die von AWS Resilience Hub intern AWS (z. B. Amazon CloudWatch) oder extern empfohlen werden AWS. Die in den Alarmen angegebenen Standardwerte basieren auf den bewährten Methoden, die bei der Erstellung dieser Alarme verwendet wurden.

Themen

Erstellung von Alarmen anhand der Betriebsempfehlungen

AWS Resilience Hub erstellt eine AWS CloudFormation Vorlage, die Details zur Erstellung der ausgewählten Alarme in Amazon enthält CloudWatch. Nachdem die Vorlage generiert wurde, können

Sie über Amazon S3 darauf zugreifenURL, sie herunterladen und in Ihre Code-Pipeline aufnehmen oder über die AWS CloudFormation Konsole einen Stack erstellen.

Um einen Alarm auf der Grundlage von AWS Resilience Hub Empfehlungen zu erstellen, müssen Sie eine AWS CloudFormation Vorlage für die empfohlenen Alarme erstellen und sie in Ihre Codebasis aufnehmen.

Um Alarme in Betriebsempfehlungen zu erstellen

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Wählen Sie unter Anwendungen Ihre Anwendung aus.
3. Wählen Sie den Tab Assessments aus.

   In der Tabelle mit den Resilienzbewertungen können Sie Ihre Bewertungen anhand der folgenden Informationen identifizieren:

   - Name — Name der Bewertung, die Sie zum Zeitpunkt der Erstellung bereitgestellt hatten.
   - Status — Gibt den Ausführungsstatus der Bewertung an.
   - Konformitätsstatus — Gibt an, ob die Bewertung der Ausfallsicherheitsrichtlinie entspricht.
   - Status der Resilienz — Gibt an, ob Ihre Anwendung im Vergleich zur vorherigen erfolgreichen Bewertung abweicht oder nicht.
   - App-Version — Version Ihrer Anwendung.
   - Aufrufer — Gibt die Rolle an, die die Bewertung aufgerufen hat.
   - Startzeit — Gibt die Startzeit der Bewertung an.
   - Endzeit — Gibt die Endzeit der Prüfung an.
   - ARN— Der Amazon-Ressourcenname (ARN) der Bewertung.
4. Wählen Sie eine Bewertung aus der Tabelle mit den Resilienzbewertungen aus. Wenn Sie noch keine Bewertung haben, schließen Sie das Verfahren unter ab the section called “Durchführung von Resilienzbewertungen” und kehren Sie dann zu diesem Schritt zurück.
5. Wählen Sie Betriebsempfehlungen aus.
6. Falls nicht standardmäßig ausgewählt, wählen Sie die Registerkarte Alarme.

   In der Tabelle „Alarme“ können Sie die empfohlenen Alarme anhand der folgenden Angaben identifizieren:

   - Name — Name des Alarms, den Sie für Ihre Anwendung festgelegt haben.

- Beschreibung — Beschreibt das Ziel des Alarms.
- Status — Zeigt den aktuellen Implementierungsstatus der CloudWatch Amazon-Alarme an.

  In dieser Spalte wird einer der folgenden Werte angezeigt:

  - Implementiert — Zeigt an, dass die von empfohlenen Alarme in Ihrer Anwendung implementiert AWS Resilience Hub sind. Wenn Sie die unten stehende Zahl auswählen, wird die Alarmtabelle so gefiltert, dass alle empfohlenen Alarme angezeigt werden, die in Ihrer Anwendung implementiert sind.
  - Nicht implementiert — Zeigt an, dass die von empfohlenen Alarme in Ihrer Anwendung enthalten, aber nicht implementiert AWS Resilience Hub sind. Wenn Sie die unten stehende Zahl auswählen, wird die Alarmtabelle so gefiltert, dass alle empfohlenen Alarme angezeigt werden, die in Ihrer Anwendung nicht implementiert sind.
  - Ausgeschlossen — Zeigt an, dass die von empfohlenen Alarme aus Ihrer Anwendung ausgeschlossen AWS Resilience Hub sind. Wenn Sie die unten stehende Zahl auswählen, wird die Alarmtabelle so gefiltert, dass alle empfohlenen Alarme angezeigt werden, die aus Ihrer Anwendung ausgeschlossen sind. Weitere Informationen zum Ein- und Ausschließen von empfohlenen Alarmen finden Sie unter Betriebsempfehlungen einbeziehen oder ausschließen.
  - Inaktiv — Zeigt an, dass die Alarme bei Amazon bereitgestellt wurden CloudWatch, der Status DATA in Amazon jedoch auf INSUFFICIENT_ gesetzt ist CloudWatch. Wenn Sie die unten stehende Zahl auswählen, wird die Alarmtabelle so gefiltert, dass alle implementierten und inaktiven Alarme angezeigt werden.
- Konfiguration — Gibt an, ob noch ausstehende Konfigurationsabhängigkeiten bestehen, die behoben werden müssen.
- Typ — Gibt die Art des Alarms an.
- AppComponent— Zeigt die Anwendungskomponenten (AppComponents) an, die diesem Alarm zugeordnet sind.
- Referenz-ID — Gibt den logischen Bezeichner des AWS CloudFormation Stack-Ereignisses in an AWS CloudFormation.
- Empfehlungs-ID — Gibt den logischen Bezeichner der AWS CloudFormation Stack-Ressource in an AWS CloudFormation.

7. Um die Alarmempfehlungen in der Alarmentabelle nach einem bestimmten Status zu filtern, wählen Sie auf der Registerkarte Alarme eine Zahl unterhalb derselben aus.

8. Wählen Sie die empfohlenen Alarme aus, die Sie für Ihre Anwendung einrichten möchten, und wählen Sie CloudFormation Vorlage erstellen.
9. Im Dialogfeld CloudFormation Vorlage erstellen können Sie den automatisch generierten Namen verwenden oder einen Namen für die AWS CloudFormation Vorlage in das Feld CloudFormation Vorlagenname eingeben.
10. Wählen Sie Create (Erstellen) aus. Das Erstellen der AWS CloudFormation Vorlage kann bis zu einigen Minuten dauern.

    Gehen Sie wie folgt vor, um die Empfehlungen in Ihre Codebasis aufzunehmen.

Um die AWS Resilience Hub Empfehlungen in Ihre Codebasis aufzunehmen

1. Wählen Sie den Tab Vorlagen, um die Vorlage anzuzeigen, die Sie gerade erstellt haben. Sie können Ihre Vorlagen wie folgt identifizieren:
   - Name — Name der Bewertung, die Sie zum Zeitpunkt der Erstellung bereitgestellt hatten.
   - Status — Gibt den Ausführungsstatus der Bewertung an.
   - Typ — Gibt die Art der Betriebsempfehlung an.
   - Format — Gibt das Format (JSON/Text) an, in dem die Vorlage erstellt wurde.
   - Startzeit — Gibt die Startzeit der Prüfung an.
   - Endzeit — Gibt die Endzeit der Prüfung an.
   - ARN— Die ARN der Vorlage
2. Wählen Sie unter Vorlagendetails den Link unter Templates S3 Path, um das Vorlagenobjekt in der Amazon S3 S3-Konsole zu öffnen.
3. Wählen Sie in der Amazon S3 S3-Konsole in der Tabelle Objekte den SOP Ordnerlink aus.
4. Um den Amazon S3 S3-Pfad zu kopieren, aktivieren Sie das Kontrollkästchen vor der JSON Datei und wählen Sie Kopieren URL.
5. Erstellen Sie einen AWS CloudFormation Stack von der AWS CloudFormation Konsole aus. Weitere Informationen zum Erstellen eines AWS CloudFormation Stacks finden Sie unterhttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Bei der Erstellung des AWS CloudFormation Stacks müssen Sie den Amazon S3-Pfad angeben, den Sie aus dem vorherigen Schritt kopiert haben.

Alarme anzeigen

Sie können alle aktiven Alarme anzeigen, die Sie zur Überwachung der Ausfallsicherheit Ihrer Anwendungen eingerichtet haben. AWS Resilience Hub verwendet eine AWS CloudFormation Vorlage zum Speichern von Alarmdetails, die wiederum für die Erstellung der Alarme in Amazon CloudWatch verwendet werden. Sie können mit Amazon S3 URL auf die AWS CloudFormation Vorlage zugreifen und sie herunterladen und in Ihre Code-Pipeline einfügen oder über die AWS CloudFormation Konsole einen Stack erstellen.

Um Alarme vom Dashboard aus anzuzeigen, wählen Sie im linken Navigationsmenü Dashboard aus. In der Tabelle „Implementierte Alarme“ können Sie die implementierten Alarme anhand der folgenden Informationen identifizieren:

- Betroffene Anwendung — Name der Anwendungen, die diesen Alarm implementiert haben.
- Aktive Alarme — Gibt die Anzahl der aktiven Alarme an, die von den Anwendungen ausgelöst wurden.
- FISin Bearbeitung — Zeigt das AWS FIS Experiment an, das derzeit für Ihre Anwendung ausgeführt wird.

Um die in Ihrer Anwendung implementierten Alarme anzuzeigen

1. Wählen Sie im linken Navigationsmenü Anwendungen.
2. Wählen Sie eine Anwendung aus der Tabelle Anwendungen aus.
3. Auf der Seite mit der Anwendungsübersicht werden in der Tabelle Implementierte Alarme alle empfohlenen Alarme angezeigt, die in Ihrer Anwendung implementiert sind.

   Um in der Tabelle Implementierte Alarme nach einem bestimmten Alarm zu suchen, wählen Sie im Feld Alarme nach Text, Eigenschaft oder Wert suchen eines der folgenden Felder aus, wählen Sie eine Operation aus, und geben Sie dann einen Wert ein.

   - Alarmname — Name des Alarms, den Sie für Ihre Anwendung festgelegt haben.
   - Beschreibung — Beschreibt das Ziel des Alarms.
   - Status — Zeigt den aktuellen Implementierungsstatus des CloudWatch Amazon-Alarms an.

     In dieser Spalte wird einer der folgenden Werte angezeigt:

     - Implementiert — Zeigt an, dass die von empfohlenen Alarme in Ihrer Anwendung implementiert AWS Resilience Hub sind. Wählen Sie die unten stehende Zahl aus, um alle

empfohlenen und implementierten Alarme auf der Registerkarte Betriebsempfehlungen anzuzeigen.

- Nicht implementiert — Zeigt an, dass die von empfohlenen Alarme in Ihrer Anwendung enthalten, aber nicht implementiert AWS Resilience Hub sind. Wählen Sie die unten stehende Zahl aus, um alle empfohlenen und nicht implementierten Alarme auf der Registerkarte Betriebsempfehlungen anzuzeigen.
- Ausgeschlossen — Zeigt an, dass die von empfohlenen Alarme aus Ihrer Anwendung ausgeschlossen AWS Resilience Hub sind. Wählen Sie die unten stehende Zahl aus, um alle empfohlenen und ausgeschlossenen Alarme auf der Registerkarte Betriebsempfehlungen anzuzeigen. Weitere Informationen zum Ein- und Ausschließen von empfohlenen Alarmen finden Sie unter Betriebsempfehlungen einbeziehen oder ausschließen.
- Inaktiv — Zeigt an, dass die Alarme bei Amazon bereitgestellt wurden CloudWatch, der Status DATA in Amazon jedoch auf INSUFFICIENT_ gesetzt ist CloudWatch. Wählen Sie die unten stehende Zahl aus, um alle implementierten und inaktiven Alarme auf der Registerkarte Betriebsempfehlungen anzuzeigen.

- Quellvorlage — Stellt den Amazon-Ressourcennamen (ARN) des AWS CloudFormation Stacks bereit, der die Alarmdetails enthält.
- Ressource — Zeigt die Ressourcen an, an die dieser Alarm angehängt ist und für die er implementiert wurde.
- Metrik — Zeigt die CloudWatch Amazon-Metrik an, die dem Alarm zugewiesen wurde. Weitere Informationen zu CloudWatch Amazon-Metriken finden Sie unter Amazon CloudWatch Metrics.
- Letzte Änderung — Zeigt das Datum und die Uhrzeit der letzten Änderung eines Alarms an.

Um die empfohlenen Alarme aus Bewertungen einzusehen

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Wählen Sie eine Anwendung aus der Tabelle Anwendungen aus.

   Um nach einer Anwendung zu suchen, geben Sie den Namen der Anwendung in das Feld Anwendungen suchen ein.
3. Wählen Sie die Registerkarte Assessments.

   In der Tabelle mit den Resilienzbewertungen können Sie Ihre Bewertungen anhand der folgenden Informationen identifizieren:

- Name — Name der Bewertung, die Sie zum Zeitpunkt der Erstellung bereitgestellt hatten.
- Status — Gibt den Ausführungsstatus der Bewertung an.
- Konformitätsstatus — Gibt an, ob die Bewertung der Ausfallsicherheitsrichtlinie entspricht.
- Status der Resilienz — Gibt an, ob Ihre Anwendung im Vergleich zur vorherigen erfolgreichen Bewertung abweicht oder nicht.
- App-Version — Version Ihrer Anwendung.
- Aufrufer — Gibt die Rolle an, die die Bewertung aufgerufen hat.
- Startzeit — Gibt die Startzeit der Bewertung an.
- Endzeit — Gibt die Endzeit der Prüfung an.
- ARN— Der Amazon-Ressourcenname (ARN) der Bewertung.

4. Wählen Sie eine Bewertung aus der Tabelle mit den Resilienzbewertungen aus.
5. Wählen Sie die Registerkarte Betriebsempfehlungen aus.
6. Falls nicht standardmäßig ausgewählt, wählen Sie die Registerkarte Alarme.

   In der Tabelle „Alarme“ können Sie die empfohlenen Alarme anhand der folgenden Angaben identifizieren:

   - Name — Name des Alarms, den Sie für Ihre Anwendung festgelegt haben.
   - Beschreibung — Beschreibt das Ziel des Alarms.
   - Status — Zeigt den aktuellen Implementierungsstatus der CloudWatch Amazon-Alarme an.

     In dieser Spalte wird einer der folgenden Werte angezeigt:

     - Implementiert — Zeigt an, dass der Alarm in Ihrer Anwendung implementiert ist. Wenn Sie die unten stehende Zahl auswählen, wird die Alarmtabelle so gefiltert, dass alle empfohlenen Alarme angezeigt werden, die in Ihrer Anwendung implementiert sind.
     - Nicht implementiert — Zeigt an, dass der Alarm nicht implementiert oder in Ihrer Anwendung enthalten ist. Wenn Sie die unten stehende Zahl auswählen, wird die Alarmtabelle so gefiltert, dass alle empfohlenen Alarme angezeigt werden, die in Ihrer Anwendung nicht implementiert sind.
     - Ausgeschlossen — Zeigt an, dass der Alarm aus der Anwendung ausgeschlossen ist. Wenn Sie die unten stehende Zahl auswählen, wird die Alarmtabelle so gefiltert, dass alle empfohlenen Alarme angezeigt werden, die von Ihrer Anwendung ausgeschlossen sind. Weitere Informationen zum Ein- und Ausschließen von empfohlenen Alarmen finden Sie unterthe section called “Einschließlich oder ohne betriebliche Empfehlungen”.

    - Inaktiv — Zeigt an, dass die Alarme bei Amazon bereitgestellt wurden CloudWatch, der Status DATA in Amazon jedoch auf INSUFFICIENT_ gesetzt ist CloudWatch. Wenn Sie die unten stehende Zahl auswählen, wird die Alarmtabelle so gefiltert, dass alle implementierten und inaktiven Alarme angezeigt werden.
- Konfiguration — Gibt an, ob noch ausstehende Konfigurationsabhängigkeiten bestehen, die behoben werden müssen.
- Typ — Gibt die Art des Alarms an.
- AppComponent— Zeigt die Anwendungskomponenten (AppComponents) an, die diesem Alarm zugeordnet sind.
- Referenz-ID — Gibt den logischen Bezeichner des AWS CloudFormation Stack-Ereignisses in an AWS CloudFormation.
- Empfehlungs-ID — Gibt den logischen Bezeichner der AWS CloudFormation Stack-Ressource in an AWS CloudFormation.

Verwaltung von Standardarbeitsanweisungen

Bei einer Standardarbeitsanweisung (SOP) handelt es sich um eine Reihe von Schritten, mit denen Sie Ihre Anwendung im Falle eines Ausfalls oder Alarms effizient wiederherstellen können. Bereiten Sie Ihre SOPs im Voraus vor, testen und messen Sie sie, um eine zeitnahe Wiederherstellung im Falle eines Betriebsausfalls sicherzustellen.

AWS Resilience Hub Empfiehlt auf der Grundlage Ihrer Anwendungskomponenten die SOPs, die Sie vorbereiten sollten. AWS Resilience Hub arbeitet mit Systems Manager zusammen, um die Schritte Ihrer SOPs zu automatisieren, indem es eine Reihe von SSM-Dokumenten bereitstellt, die Sie als Grundlage für diese SOPs verwenden können.

AWS Resilience Hub Kann beispielsweise eine SOP zum Hinzufügen von Festplattenspeicher auf der Grundlage eines vorhandenen SSM-Automation-Dokuments empfehlen. Um dieses SSM-Dokument auszuführen, benötigen Sie eine bestimmte IAM-Rolle mit den richtigen Berechtigungen. AWS Resilience Hub erstellt Metadaten in Ihrer Anwendung, die angeben, welches SSM-Automatisierungsdokument im Falle eines Festplattenmangels ausgeführt werden soll und welche IAM-Rolle für die Ausführung dieses SSM-Dokuments erforderlich ist. Diese Metadaten werden dann in einem SSM-Parameter gespeichert.

Neben der Konfiguration der SSM-Automatisierung empfiehlt es sich auch, sie mit einem AWS FIS Experiment zu testen. Daher bietet es AWS Resilience Hub auch ein AWS FIS Experiment, bei dem

das SSM-Automatisierungsdokument aufgerufen wird. Auf diese Weise können Sie Ihre Anwendung proaktiv testen, um sicherzustellen, dass die von Ihnen erstellte SOP die beabsichtigte Aufgabe erfüllt.

AWS Resilience Hub stellt die Empfehlungen in Form einer AWS CloudFormation Vorlage bereit, die Sie Ihrer Anwendungscodebasis hinzufügen können. Diese Vorlage bietet:

- Die IAM-Rolle mit den für die Ausführung der SOP erforderlichen Berechtigungen.
- Ein AWS FIS Experiment, mit dem Sie die SOP testen können.
- Ein SSM-Parameter, der Anwendungsmetadaten enthält, die angeben, welches SSM-Dokument und welche IAM-Rolle als SOP ausgeführt werden sollen und auf welcher Ressource. Zum Beispiel: `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`.

Das Erstellen einer SOP erfordert möglicherweise einige Versuche und Irrtümer. Es ist ein guter Anfang, eine Resilienzanalyse für Ihre Anwendung durchzuführen und anhand der AWS Resilience Hub Empfehlungen eine AWS CloudFormation Vorlage zu generieren. Verwenden Sie die AWS CloudFormation Vorlage, um einen AWS CloudFormation Stack zu generieren, und verwenden Sie dann die SSM-Parameter und deren Standardwerte in Ihrer SOP. Führen Sie die SOP aus und sehen Sie, welche Verbesserungen Sie vornehmen müssen.

Da für alle Anwendungen unterschiedliche Anforderungen gelten, reicht die Standardliste der AWS Resilience Hub bereitgestellten SSM-Dokumente nicht für alle Ihre Anforderungen aus. Sie können jedoch die SSM-Standarddokumente kopieren und sie als Grundlage verwenden, um Ihre eigenen benutzerdefinierten Dokumente zu erstellen, die auf Ihre Anwendung zugeschnitten sind. Sie können auch Ihre eigenen völlig neuen SSM-Dokumente erstellen. Wenn Sie Ihre eigenen SSM-Dokumente erstellen, anstatt die Standardeinstellungen zu ändern, müssen Sie sie mit SSM-Parametern verknüpfen, damit das richtige SSM-Dokument aufgerufen wird, wenn die SOP ausgeführt wird.

Wenn Sie Ihre SOP fertiggestellt haben, indem Sie die erforderlichen SSM-Dokumente erstellt und die Parameter- und Dokumentzuordnungen nach Bedarf aktualisiert haben, fügen Sie die SSM-Dokumente direkt zu Ihrer Codebasis hinzu und nehmen dort alle nachfolgenden Änderungen oder Anpassungen vor. Auf diese Weise stellen Sie jedes Mal, wenn Sie Ihre Anwendung bereitstellen, auch die meisten SOP bereit. up-to-date

Themen

- Verwenden Sie ein benutzerdefiniertes SSM-Dokument anstelle des Standarddokuments
- SOPs testen
- Standardarbeitsanweisungen anzeigen

Erstellung einer SOP auf der Grundlage von AWS Resilience Hub Empfehlungen

Um eine SOP auf der Grundlage von AWS Resilience Hub Empfehlungen zu erstellen, benötigen Sie eine AWS Resilience Hub Anwendung, der eine Ausfallsicherheitsrichtlinie zugeordnet ist, und Sie müssen eine Resilienzbewertung für diese Anwendung durchgeführt haben. Die Resilienzbewertung generiert die Empfehlungen für Ihre SOP.

Um eine SOP auf der Grundlage von AWS Resilience Hub Empfehlungen zu erstellen, müssen Sie eine AWS CloudFormation Vorlage für die empfohlenen SOPs erstellen und diese in Ihre Codebasis aufnehmen.

Erstellen Sie eine AWS CloudFormation Vorlage für die SOP-Empfehlungen

1. Öffnen Sie die AWS Resilience Hub Konsole.
2. Wählen Sie im Navigationsbereich Applications (Anwendungen).
3. Wählen Sie aus der Liste der Anwendungen die Anwendung aus, für die Sie eine SOP erstellen möchten.
4. Wählen Sie die Registerkarte Assessments.
5. Wählen Sie eine Bewertung aus der Tabelle mit den Resilienzbewertungen aus. Wenn Sie noch keine Bewertung haben, schließen Sie das Verfahren unter ab the section called “Durchführung von Resilienzbewertungen” und kehren Sie dann zu diesem Schritt zurück.
6. Wählen Sie unter Betriebsempfehlungen die Option Standardarbeitsanweisungen aus.
7. Wählen Sie alle SOP-Empfehlungen aus, die Sie einbeziehen möchten.
8. Wählen Sie CloudFormation Vorlage erstellen aus. Das Erstellen der AWS CloudFormation Vorlage kann bis zu einigen Minuten dauern.

   Gehen Sie wie folgt vor, um die SOP-Empfehlungen in Ihre Codebasis aufzunehmen.

Um die AWS Resilience Hub Empfehlungen in Ihre Codebasis aufzunehmen

1. Wählen Sie unter Betriebsempfehlungen die Option Vorlagen aus.

2. Wählen Sie in der Liste der Vorlagen den Namen der SOP-Vorlage aus, die Sie gerade erstellt haben.

   Sie können die SOPs, die in Ihrer Anwendung implementiert sind, anhand der folgenden Informationen identifizieren:

   - SOP-Name — Name der SOP, die Sie für Ihre Anwendung definiert haben.
   - Beschreibung — Beschreibt das Ziel der SOP.
   - SSM-Dokument — Amazon S3 S3-URL des SSM-Dokuments, das die SOP-Definition enthält.
   - Testlauf — Amazon S3 S3-URL des Dokuments, das die Ergebnisse des letzten Tests enthält.
   - Quellvorlage — Stellt den Amazon-Ressourcennamen (ARN) des AWS CloudFormation Stacks bereit, der die SOP-Details enthält.
3. Wählen Sie unter Vorlagendetails den Link in Templates S3 Path, um das Vorlagenobjekt in der Amazon S3 S3-Konsole zu öffnen.
4. Wählen Sie in der Amazon S3 S3-Konsole in der Tabelle Objekte den Link SOP-Ordner aus.
5. Um den Amazon S3 S3-Pfad zu kopieren, aktivieren Sie das Kontrollkästchen vor der JSON-Datei und wählen Sie URL kopieren.
6. Erstellen Sie einen AWS CloudFormation Stack von der AWS CloudFormation Konsole aus. Weitere Informationen zum Erstellen eines AWS CloudFormation Stacks finden Sie unterhttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Bei der Erstellung des AWS CloudFormation Stacks müssen Sie den Amazon S3-Pfad angeben, den Sie aus dem vorherigen Schritt kopiert haben.

Ein benutzerdefiniertes SSM-Dokument erstellen

Um die Wiederherstellung Ihrer Anwendung vollständig zu automatisieren, müssen Sie möglicherweise ein benutzerdefiniertes SSM-Dokument für Ihre SOP in der Systems Manager Manager-Konsole erstellen. Sie können ein vorhandenes SSM-Dokument als Grundlage ändern oder ein neues SSM-Dokument erstellen.

Ausführliche Informationen zur Verwendung von Systems Manager zum Erstellen eines SSM-Dokuments finden Sie unter Exemplarische Vorgehensweise: Verwenden von Document Builder zum Erstellen eines benutzerdefinierten Runbooks.

Informationen zur SSM-Dokumentsyntax finden Sie unter SSM-Dokumentsyntax.

Informationen zur Automatisierung von SSM-Dokumentaktionen finden Sie unter Referenz zu Systems Manager Manager-Automatisierungsaktionen.

Verwenden Sie ein benutzerdefiniertes SSM-Dokument anstelle des Standarddokuments

Um das für Ihre SOP AWS Resilience Hub vorgeschlagene SSM-Dokument durch ein von Ihnen erstelltes benutzerdefiniertes Dokument zu ersetzen, arbeiten Sie direkt in Ihrer Codebasis. Zusätzlich zum Hinzufügen Ihres neuen benutzerdefinierten SSM-Automatisierungsdokuments werden Sie auch:

1. Fügen Sie die IAM-Berechtigungen hinzu, die für die Ausführung der Automatisierung erforderlich sind.
2. Fügen Sie ein AWS FIS Experiment hinzu, um Ihr SSM-Dokument zu testen.
3. Fügen Sie einen SSM-Parameter hinzu, der auf das Automatisierungsdokument verweist, das Sie als SOP verwenden möchten.

Im Allgemeinen ist es am effizientesten, mit den vorgeschlagenen Standardwerten zu arbeiten AWS Resilience Hub und sie nach Bedarf anzupassen. Fügen Sie beispielsweise je nach Bedarf Berechtigungen für die IAM-Rolle hinzu oder entfernen Sie sie, ändern Sie den AWS FIS Versuchsaufbau so, dass er auf das neue SSM-Dokument verweist, oder ändern Sie den SSM-Parameter so, dass er auf Ihr neues SSM-Dokument verweist.

SOPs testen

Wie bereits erwähnt, empfiehlt es sich, Ihre CI/CD-Pipelines um AWS FIS Experimente zu erweitern, um Ihre SOPs regelmäßig zu testen. Dadurch wird sichergestellt, dass sie bei einem Ausfall einsatzbereit sind.

Testen Sie sowohl bereitgestellte als auch benutzerdefinierte SOPs AWS Resilience Hub.

Standardarbeitsanweisungen anzeigen

Um die implementierten SOPs von Anwendungen aus anzuzeigen

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Öffnen Sie unter Anwendungen eine Anwendung.
3. Wählen Sie die Registerkarte Standardarbeitsanweisungen.

Im Abschnitt Zusammenfassung der Standardarbeitsanweisungen wird in der Tabelle Implementierte Standardarbeitsanweisungen die Liste der SOPs angezeigt, die aus SOP-Empfehlungen generiert wurden.

Sie können Ihre SOPs wie folgt identifizieren:

- SOP-Name — Name der SOP, die Sie für Ihre Anwendung definiert haben.
- SSM-Dokument — S3-URL des Amazon EC2 Systems Manager Manager-Dokuments, das die SOP-Definition enthält.
- Beschreibung — Beschreibt das Ziel der SOP.
- Testlauf — S3-URL des Dokuments, das die Ergebnisse des letzten Tests enthält.
- Referenz-ID — Kennung der referenzierten SOP-Empfehlung.
- Ressourcen-ID — Kennung der Ressource, für die die SOP-Empfehlung implementiert wurde.

Um die empfohlenen SOPs aus Assessments einzusehen

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Wählen Sie eine Anwendung aus der Tabelle Anwendungen aus.

   Um nach einer Anwendung zu suchen, geben Sie den Namen der Anwendung in das Feld Anwendungen suchen ein.
3. Wählen Sie die Registerkarte Assessments.

   In der Tabelle mit den Resilienzbewertungen können Sie Ihre Bewertungen anhand der folgenden Informationen identifizieren:

   - Name — Name der Bewertung, die Sie zum Zeitpunkt der Erstellung bereitgestellt hatten.
   - Status — Gibt den Ausführungsstatus der Bewertung an.
   - Konformitätsstatus — Gibt an, ob die Bewertung der Ausfallsicherheitsrichtlinie entspricht.
   - Status der Resilienz — Gibt an, ob Ihre Anwendung im Vergleich zur vorherigen erfolgreichen Bewertung abweicht oder nicht.
   - App-Version — Version Ihrer Anwendung.
   - Aufrufer — Gibt die Rolle an, die die Bewertung aufgerufen hat.
   - Startzeit — Gibt die Startzeit der Bewertung an.
   - Endzeit — Gibt die Endzeit der Prüfung an.

- ARN — Der Amazon-Ressourcenname (ARN) der Bewertung.

4. Wählen Sie eine Bewertung aus der Tabelle mit den Resilienzbewertungen aus.
5. Wählen Sie die Registerkarte Betriebsempfehlungen aus.
6. Wählen Sie die Registerkarte Standardarbeitsanweisungen.

   In der Tabelle mit den Standardarbeitsanweisungen können Sie anhand der folgenden Informationen mehr über die empfohlenen SOPs erfahren:

   - Name — Name der empfohlenen SOP.
   - Beschreibung — Beschreibt das Ziel der SOP.
   - Status — Gibt den aktuellen Implementierungsstatus der SOP an. Das heißt, Implementiert, Nicht implementiert und Ausgeschlossen.
   - Konfiguration — Gibt an, ob noch ausstehende Konfigurationsabhängigkeiten bestehen, die behoben werden müssen.
   - Typ — Gibt den SOP-Typ an.
   - AppComponent— Gibt die Anwendungskomponenten (AppComponents) an, die dieser SOP zugeordnet sind. Weitere Informationen zu unterstützten AppComponents Ressourcen finden Sie unter Ressourcen in einem AppComponent gruppieren.
   - Referenz-ID — Gibt den logischen Bezeichner des AWS CloudFormation Stack-Ereignisses in an AWS CloudFormation.
   - Empfehlungs-ID — Gibt den logischen Bezeichner der AWS CloudFormation Stack-Ressource in an AWS CloudFormation.

Verwaltung von Amazon Fault Injection Service-Experimenten

In diesem Abschnitt wird beschrieben, wie Sie Amazon Fault Injection Service (AWS FIS) - Experimente in erstellen und ausführen AWS Resilience Hub. Sie führen AWS FIS Experimente durch, um die Widerstandsfähigkeit Ihrer AWS Ressourcen und die Zeit zu messen, die für die Wiederherstellung nach Anwendungen, Infrastruktur, Availability Zone und AWS-Region Vorfällen benötigt wird.

Um die Ausfallsicherheit zu messen, simulieren diese AWS FIS Experimente Störungen Ihrer Ressourcen. AWS Beispiele für Störungen sind Netzwerkfehler, Failovers, gestoppte Prozesse auf Amazon EC2 oder AWS ASG, Startwiederherstellung in Amazon RDS und Probleme mit Ihrer

Availability Zone. Wenn das AWS FIS Experiment abgeschlossen ist, können Sie abschätzen, ob eine Anwendung die im RTO-Ziel der Resilienz-Richtlinie definierten Ausfallarten überstehen kann.

Alle Experimente AWS Resilience Hub basieren auf Aktionen AWS FIS und führen diese aus AWS FIS . Bei den meisten AWS FIS Experimenten werden Automatisierungsaktionen von Systems Manager aufgerufen, um Störungen durchzuführen und die Alarme zu überwachen. Andere AWS FIS Experimente verwenden nur AWS FIS Automatisierungsaktionen, die auf bestimmte AWS Dienste zugeschnitten sind (z. B. Amazon EKS-Aktionen). Weitere Informationen zu AWS FIS Aktionen finden Sie in der AWS FIS Aktionsreferenz.

Sie können die AWS FIS Experimente in ihrem Standardstatus verwenden oder sie an Ihre Anforderungen anpassen. AWS FIS Auf Experimente kann entweder von AWS Resilience Hub (the section called “Experimente mit Fehlerinjektion anzeigen”) oder der AWS FIS Konsole (AWS FIS) aus zugegriffen werden.

Themen

- Erstellung von AWS FIS Experimenten auf der Grundlage der Betriebsempfehlungen
- Durchführung eines AWS FIS Experiments von AWS Resilience Hub
- Experimente mit Fehlerinjektion anzeigen
- Fehler beim Amazon Fault Injection Service-Experiment/Statusüberprüfung

Erstellung von AWS FIS Experimenten auf der Grundlage der Betriebsempfehlungen

AWS Resilience Hub empfiehlt, dass Sie Ihre Anwendung testen, nachdem Sie einen Bewertungsbericht erstellt haben. Sie können über den Bewertungsbericht Ihrer Anwendung auf diese Experimente zugreifen und sie ausführen.

AWS Resilience Hub bietet eine Liste von AWS FIS Experimenten, bei denen es sich um Systems Manager Manager-Dokumente mit Testparametern handelt. Wenn Sie ein AWS FIS Experiment aus der Liste auswählen, AWS Resilience Hub erstellt eine AWS CloudFormation Vorlage mit den Parametern, die Sie im Systems Manager Manager-Dokument definiert haben. Nach der Erstellung des AWS CloudFormation Stacks können Sie Ihre bereitgestellten AWS FIS Experimente für Ihre Anwendung sehen.

Die AWS CloudFormation Vorlage besteht aus einer IAM-Rolle für jedes Systems Manager Manager-Dokument mit den für die Ausführung erforderlichen Mindestberechtigungen.

Um ein AWS FIS Experiment auf der Grundlage von AWS Resilience Hub Empfehlungen zu erstellen, müssen Sie eine AWS CloudFormation Vorlage für die empfohlenen Tests erstellen und diese in Ihre Codebasis aufnehmen.

Um eine AWS CloudFormation Vorlage für das AWS FIS Experiment zu erstellen

1. Öffne die AWS Resilience Hub Konsole.
2. Wählen Sie im Navigationsbereich Applications (Anwendungen).
3. Wählen Sie aus der Liste der Anwendungen die Anwendung aus, für die Sie einen Test erstellen möchten.
4. Wählen Sie die Registerkarte Assessments.
5. Wählen Sie eine Bewertung aus der Tabelle mit den Resilienzbewertungen aus. Wenn Sie noch keine Bewertung haben, schließen Sie das Verfahren unter ab the section called “Durchführung von Resilienzbewertungen” und kehren Sie dann zu diesem Schritt zurück.
6. Wählen Sie unter Betriebsempfehlungen die Option Experimente zur Fehlerinjektion aus.
7. Wählen Sie alle Tests aus, die Sie einbeziehen möchten.
8. Wählen Sie CloudFormation Vorlage erstellen. Das Erstellen der AWS CloudFormation Vorlage kann bis zu einigen Minuten dauern.
9. Wählen Sie Templates (Vorlagen).

   Sie können die neu erstellte AWS CloudFormation Vorlage in der Tabelle Vorlagen einsehen.

   Gehen Sie wie folgt vor, um die Empfehlungen in Ihre Codebasis aufzunehmen.

Um die AWS Resilience Hub Empfehlungen in Ihre Codebasis aufzunehmen

1. Wählen Sie unter Betriebsempfehlungen die Option Vorlagen aus.
2. Wählen Sie in der Liste der Vorlagen den Namen der AWS FIS Experimentvorlage aus, die Sie gerade erstellt haben.

   Anhand der folgenden Informationen können Sie die Tests identifizieren, die in Ihrer Anwendung implementiert sind:

   - Testname — Name des Tests, den Sie für Ihre Anwendung erstellt haben.
   - Beschreibung — Beschreibt das Ziel des Tests.
   - Status — Gibt den aktuellen Implementierungsstatus des Tests an.

In dieser Spalte wird einer der folgenden Werte angezeigt:

- Implementiert — Zeigt an, dass der Test in Ihrer Anwendung implementiert ist.
- Nicht implementiert — Zeigt an, dass der Test nicht implementiert oder in Ihrer Anwendung enthalten ist.
- Ausgeschlossen — Zeigt an, dass der Test aus der Anwendung ausgeschlossen ist.
- Inaktiv — Zeigt an, dass der Test zwar bereitgestellt wurde AWS FIS, aber in den letzten 30 Tagen nicht ausgeführt wurde.

- Testlauf — Amazon S3 S3-URL des Dokuments, das die Ergebnisse des letzten Tests enthält.
- Quellvorlage — Stellt den Amazon-Ressourcennamen (ARN) des AWS CloudFormation Stacks bereit, der die Experimentdetails enthält.

3. Wählen Sie unter Vorlagendetails den Link in Templates S3 Path, um das Vorlagenobjekt in der Amazon S3 S3-Konsole zu öffnen.
4. Wählen Sie in der Amazon S3 S3-Konsole in der Tabelle Objekte den Link zum Testordner aus.
5. Um den Amazon S3 S3-Pfad zu kopieren, aktivieren Sie das Kontrollkästchen vor der JSON-Datei und wählen Sie URL kopieren.
6. Erstellen Sie einen AWS CloudFormation Stack von der AWS CloudFormation Konsole aus. Weitere Informationen zum Erstellen eines AWS CloudFormation Stacks finden Sie unterhttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Bei der Erstellung des AWS CloudFormation Stacks müssen Sie den Amazon S3-Pfad angeben, den Sie aus dem vorherigen Schritt kopiert haben.

Durchführung eines AWS FIS Experiments von AWS Resilience Hub

In Ihrer Anwendung müssen Sie zunächst anhand der Betriebsempfehlungen eine AWS FIS Versuchsvorlage erstellen, bevor Sie das AWS FIS Experiment ausführen AWS Resilience Hub können.

Um ein AWS FIS Experiment zu starten

1. Wählen Sie im linken Navigationsmenü Anwendungen.
2. Öffnen Sie in der Tabelle Anwendungen eine Anwendung.
3. Wählen Sie die Registerkarte „Experimente zur Fehlerinjektion“.

4. Wählen Sie in der Tabelle mit den Versuchsvorlagen das Optionsfeld vor der Experimentvorlage aus, mit der das Experiment erstellt wurde, das Sie ausführen möchten, und wählen Sie dann Experiment starten aus.

Um ein AWS FIS Experiment zu beenden

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Öffnen Sie in der Tabelle Anwendungen eine Anwendung.
3. Wählen Sie die Registerkarte „Experimente zur Fehlerinjektion“.
4. Wählen Sie in der Experimenttabelle das Optionsfeld vor dem Experiment aus und wählen Sie dann Experiment beenden aus.

Experimente mit Fehlerinjektion anzeigen

Sehen Sie sich unter die AWS FIS Experimente an AWS Resilience Hub, die Sie eingerichtet haben, um die Widerstandsfähigkeit Ihrer AWS Ressourcen und die Zeit zu messen, die für die Wiederherstellung nach Anwendungen, Infrastruktur, Availability Zone und AWS-Region Vorfällen benötigt wird.

Um die AWS FIS Experimente vom Dashboard aus anzuzeigen, wählen Sie im linken Navigationsmenü die Option Dashboard aus. In der Tabelle mit den Experimenten können Sie die durchgeführten AWS FIS Experimente anhand der folgenden Informationen identifizieren:

- Experiment-ID — Kennung des AWS FIS Experiments.
- Experimentvorlagen-ID — Kennung der AWS FIS Experimentvorlage, die zur Erstellung des AWS FIS Experiments verwendet wurde.
- Quellvorlage — Stellt den Amazon-Ressourcennamen (ARN) des AWS CloudFormation Stacks bereit, der Details des AWS FIS Experiments enthält.
- Status — Gibt an, ob das AWS FIS Experiment erfolgreich abgeschlossen wurde oder nicht.

Um die durchgeführten AWS FIS Experimente in Anwendungen einzusehen

1. Wählen Sie im linken Navigationsmenü Anwendungen.
2. Öffnen Sie in der Tabelle Anwendungen eine Anwendung.
3. Wählen Sie Experimente zur Fehlerinjektion aus.

4. Wählen Sie die Registerkarte Experiment.

   Auf der Registerkarte „Experiment“ finden Sie in der Tabelle „ AWS FIS Experiment“ eine Liste der aktiven Experimente.

   In der Tabelle Experimente können Sie das durchgeführte AWS FIS Experiment anhand der folgenden Informationen identifizieren:

   - Testname — Name des von AWS Resilience Hub empfohlenen Tests, der zur Erstellung des AWS FIS Experiments verwendet wurde.
   - Experiment-ID — Kennung des AWS FIS Experiments.
   - Beschreibung — Beschreibt das Ziel des AWS FIS Experiments.
   - Erstellungszeit — Datum und Uhrzeit der Erstellung des AWS FIS Experiments.
   - Uhrzeit der letzten Aktualisierung — Datum und Uhrzeit der letzten Aktualisierung des AWS FIS Experiments.
   - Quellvorlage — Stellt den Amazon-Ressourcennamen (ARN) des AWS CloudFormation Stacks bereit, der Details des AWS FIS Experiments enthält.

Um die empfohlenen Experimente aus Assessments einzusehen

1. Wählen Sie im linken Navigationsmenü Anwendungen.
2. Wählen Sie eine Anwendung aus der Tabelle Anwendungen aus.

   Um nach einer Anwendung zu suchen, geben Sie den Namen der Anwendung in das Feld Anwendungen suchen ein.
3. Wählen Sie die Registerkarte Assessments.

   In der Tabelle mit den Resilienzbewertungen können Sie Ihre Bewertungen anhand der folgenden Informationen identifizieren:

   - Name — Name der Bewertung, die Sie zum Zeitpunkt der Erstellung bereitgestellt hatten.
   - Status — Gibt den Ausführungsstatus der Bewertung an.
   - Konformitätsstatus — Gibt an, ob die Bewertung der Ausfallsicherheitsrichtlinie entspricht.
   - Status der Resilienz — Gibt an, ob Ihre Anwendung im Vergleich zur vorherigen erfolgreichen Bewertung abweicht oder nicht.
   - App-Version — Version Ihrer Anwendung.

- Aufrufer — Gibt die Rolle an, die die Bewertung aufgerufen hat.
- Startzeit — Gibt die Startzeit der Bewertung an.
- Endzeit — Gibt die Endzeit der Prüfung an.
- ARN — Der Amazon-Ressourcenname (ARN) der Bewertung.

4. Wählen Sie eine Bewertung aus der Tabelle mit den Resilienzbewertungen aus.
5. Wählen Sie die Registerkarte Betriebsempfehlungen aus.
6. Wählen Sie die Registerkarte „Experimente zur Fehlerinjektion“.

   In der Tabelle mit den Vorlagen für Fault-Injection-Experimente können Sie anhand der folgenden Informationen mehr über die empfohlenen Tests erfahren:

   - Name — Name des empfohlenen Tests.
   - Beschreibung — Beschreibt das Ziel des Tests.
   - Status — Gibt den aktuellen Implementierungsstatus des Tests an.

     In dieser Spalte wird einer der folgenden Werte angezeigt:

     - Implementiert — Zeigt an, dass der Test in Ihrer Anwendung implementiert ist.
     - Nicht implementiert — Zeigt an, dass der Test nicht implementiert oder in Ihrer Anwendung enthalten ist.
     - Ausgeschlossen — Zeigt an, dass der Test aus der Anwendung ausgeschlossen ist.
     - Inaktiv — Zeigt an, dass der Test zwar bereitgestellt wurde AWS FIS, aber in den letzten 30 Tagen nicht ausgeführt wurde.
   - Konfiguration — Gibt an, ob noch ausstehende Konfigurationsabhängigkeiten bestehen, die behoben werden müssen.
   - Typ — Gibt die Art des Tests an.
   - AppComponent— Gibt die Anwendungskomponenten (AppComponents) an, die diesem Test zugeordnet sind. Weitere Informationen zu unterstützten AppComponents Ressourcen finden Sie unter Ressourcen in einem AppComponent gruppieren.
   - Risiko — Gibt die Risikostufe des fehlgeschlagenen Tests an. Die Risikostufen werden mit Hoch, Mittel und Niedrig angegeben, um jeweils ein hohes, mittleres und niedriges Risikoniveau anzugeben.
   - Referenz-ID — Gibt den logischen Bezeichner des AWS CloudFormation Stack-Ereignisses in an AWS CloudFormation.

- Empfehlungs-ID — Gibt den logischen Bezeichner der AWS CloudFormation Stack-Ressource in an AWS CloudFormation.

Fehler beim Amazon Fault Injection Service-Experiment/Statusüberprüfung

AWS Resilience Hub ermöglicht es Ihnen, den Status Ihres Experiments zu verfolgen, das Sie gestartet haben. Weitere Informationen finden Sie im Verfahren So sehen Sie sich die empfohlenen Experimente aus Bewertungen an unterthe section called “Experimente mit Fehlerinjektion anzeigen”.

Themen

- Analysieren der AWS FIS Versuchsausführung mit AWS Systems Manager
- AWS FIS Experimentierfehler beim Testen von Kubernetes-Pods, die in Ihren Amazon Elastic Kubernetes Service Service-Clustern ausgeführt werden

Analysieren der AWS FIS Versuchsausführung mit AWS Systems Manager

Nach dem Ausführen eines AWS FIS Experiments können Sie die Ausführungsdetails im AWS Systems Manager anzeigen.

1. Gehen Sie zu CloudTrail> Ereignisverlauf.
2. Filtern Sie Ereignisse anhand der Experiment-ID nach dem Benutzernamen.
3. Sehen Sie sich den StartAutomationExecution Eintrag an. Die Anforderungs-ID ist die SSM-Automatisierungs-ID.
4. Gehen Sie zu AWS Systems Manager > Automation.
5. Filtern Sie mithilfe der SSM-Automatisierungs-ID nach der Ausführungs-ID und sehen Sie sich die Automatisierungsdetails an.

   Sie können die Ausführung mit jeder Systems Manager Manager-Automatisierung analysieren. Weitere Informationen finden Sie im AWS Systems Manager Automation Automation-Benutzerhandbuch. Die Eingabeparameter für die Ausführung werden im Abschnitt Eingabeparameter der Ausführungsdetails angezeigt und enthalten optionale Parameter, die im AWS FIS Experiment nicht vorkommen.

   Informationen zum Schrittstatus und zu anderen Schrittdetails finden Sie, indem Sie innerhalb der Ausführungsschritte zu bestimmten Schritten aufschlüsseln.

Häufige Fehler

Die folgenden Fehler treten häufig bei der Ausführung eines Bewertungsberichts auf:

- Die Alarmvorlage wurde nicht bereitgestellt, bevor das Test-/SOP-Experiment ausgeführt wurde. Dies führt zu einer Fehlermeldung während des Automatisierungsschritts.
  - Fehlermeldung: `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.`
  - Behebung: Stellen Sie sicher, dass der entsprechende Alarm ausgegeben und die daraus resultierende Vorlage bereitgestellt wird, bevor Sie das Fault-Injection-Experiment erneut ausführen.
- Fehlende Berechtigungen in der Ausführungsrolle. Diese Fehlermeldung tritt auf, wenn der angegebenen Ausführungsrolle eine Berechtigung fehlt, und erscheint in den Schrittdetails.
  - Fehlermeldung:`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.`
  - Behebung: Stellen Sie sicher, dass Sie die richtige Ausführungsrolle angegeben haben. Wenn dies geschehen ist, fügen Sie die erforderliche Berechtigung hinzu und führen Sie die Bewertung erneut durch.
- Die Ausführung war erfolgreich, hatte aber nicht das erwartete Ergebnis. Dies ist auf falsche Parameter oder ein internes Automatisierungsproblem zurückzuführen.
  - Fehlermeldung: Die Ausführung war erfolgreich, sodass keine Fehlermeldung angezeigt wird.
  - Behebung: Überprüfen Sie die Eingabeparameter und sehen Sie sich die ausgeführten Schritte an, wie im Abschnitt Ausführung des AWS FIS Experiments analysieren beschrieben, bevor Sie die einzelnen Schritte auf erwartete Eingaben und Ausgaben untersuchen.

AWS FIS Experimentierfehler beim Testen von Kubernetes-Pods, die in Ihren Amazon Elastic Kubernetes Service Service-Clustern ausgeführt werden

Im Folgenden sind beim Testen von Kubernetes-Pods, die in Ihren Amazon EKS-Clustern ausgeführt werden, häufig Fehler bei Amazon Elastic Kubernetes Service (Amazon EKS) aufgetreten:

- Falsche Konfiguration der IAM-Rollen für AWS FIS Experimente oder des Kubernetes-Servicekontos.
  - Fehlermeldungen:
    - `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.`
  - Behebung: Überprüfen Sie Folgendes.
    - Stellen Sie sicher, dass Sie die Anweisungen unter Verwenden der AWS FIS`aws:eks:pod` Aktionen befolgt haben.
    - Stellen Sie sicher, dass Sie ein Kubernetes-Dienstkonto mit den erforderlichen RBAC-Berechtigungen und dem richtigen Namespace erstellt und konfiguriert haben.
    - Stellen Sie sicher, dass Sie die angegebene IAM-Rolle (siehe Ausgabe des AWS CloudFormation Teststapels) dem Kubernetes-Benutzer zugeordnet haben.
- AWS FIS Pod konnte nicht gestartet werden: Die maximale Anzahl ausgefallener Sidecar-Container wurde erreicht. Dies passiert normalerweise, wenn der Speicher nicht ausreicht, um den AWS FIS Sidecar-Container auszuführen.
  - Fehlermeldung:. `Unable to heartbeat FIS Pod: Max failed sidecar containers reached`
  - Behebung: Eine Möglichkeit, diesen Fehler zu vermeiden, besteht darin, den Zielauslastungsprozentsatz zu reduzieren, um ihn an den verfügbaren Arbeitsspeicher oder die verfügbare CPU anzupassen.
- Die Alarmbestätigung schlug zu Beginn des Experiments fehl. Dieser Fehler tritt auf, weil der zugehörige Alarm keinen Datenpunkt hat.
  - Fehlermeldung:. `Assertion failed for the following alarms` Listet alle Alarme auf, bei denen die Assertion fehlgeschlagen ist.
  - Behebung: Stellen Sie sicher, dass Container Insights für die Alarme korrekt installiert ist und der Alarm nicht aktiviert ist (im `ALARM` Status).

Resilienzwerte verstehen

In diesem Abschnitt wird beschrieben, wie AWS Resilience Hub die Anwendungsbereitschaft anhand verschiedener Unterbrechungsszenarien quantifiziert wird.

AWS Resilience Hub stellt einen Resilienz-Score bereit, der den Zustand der Ausfallsicherheit der Anwendung wiedergibt. Diese Bewertung gibt an, wie genau die Anwendung unseren Empfehlungen zur Einhaltung der Stabilitätsrichtlinien, Alarme, Standardarbeitsanweisungen (SOPs) und Tests für die Anwendung entspricht. Basierend auf der Art der Ressourcen, die die Anwendung verwendet, werden Alarme und eine Reihe von Tests für jeden Störungstyp AWS Resilience Hub empfohlen. SOPs

Die höchste Resilienz-Punktzahl liegt bei 100 Punkten. Um die bestmögliche Punktzahl oder die höchste Punktzahl zu erreichen, müssen Sie alle empfohlenen Alarme und Tests in Ihrer Anwendung implementieren. SOPs AWS Resilience Hub Empfiehlt beispielsweise einen Test mit einem Alarm und einemSOP. Der Test wird ausgeführt und löst den Alarm aus und löst den zugehörigen SOP Alarm aus. Wenn sie erfolgreich ausgeführt werden und die Anwendung die Resilienz-Richtlinie erfüllt, erhält sie einen Resilienzwert von fast oder gleich 100 Punkten.

AWS Resilience Hub Bietet nach der Ausführung der ersten Bewertung die Option, betriebliche Empfehlungen aus Ihrer Anwendung auszuschließen. Um zu verstehen, wie sich die ausgeschlossenen Empfehlungen auf den Resilienzwert auswirken, müssen Sie eine neue Bewertung durchführen. Sie können die ausgeschlossenen Empfehlungen jedoch jederzeit in Ihre Anwendung aufnehmen und eine neue Bewertung durchführen. Weitere Informationen zum Ein- und Ausschließen von Alarm SOP - und Testempfehlungen finden Sie unterthe section called “Einschließlich oder ohne betriebliche Empfehlungen”.

Zugriff auf den Resiliency Score Ihrer Anwendungen

Sie können den Resilienz-Score Ihrer Anwendung anzeigen, indem Sie im Navigationsmenü Dashboard oder Anwendungen auswählen.

Über das Dashboard auf den Resilienz-Score zugreifen

1. Wählen Sie im linken Navigationsmenü Dashboard.
2. Wählen Sie unter Bewertung der Ausfallsicherheit von Anwendungen im Zeitverlauf eine oder mehrere Anwendungen aus der Dropdownliste Wählen Sie bis zu 4 Anwendungen aus.
3. Das Resilienz-Score-Diagramm zeigt den Resilienzwert für alle ausgewählten Anwendungen.

Zugriff auf den Resilienz-Score von Anwendungen aus

1. Wählen Sie im linken Navigationsmenü Anwendungen aus.
2. Öffnen Sie unter Anwendungen eine Anwendung.
3. Wählen Sie Summary (Übersicht) aus.

   Das Resilienz-Score-Diagramm zeigt den Trend der Resilienzbewertung Ihrer Anwendung über einen Zeitraum von bis zu einem Jahr. AWS Resilience Hub zeigt Aktionspunkte, Verstöße gegen die Ausfallsicherheitsrichtlinien und betriebliche Empfehlungen, die zur Verbesserung und Erreichung des höchstmöglichen Resilienzwerts umgesetzt werden müssen, und zwar anhand der folgenden Kriterien:

   - Wählen Sie die Registerkarte Aktionspunkte, um die Maßnahmen anzuzeigen, die zur Verbesserung und Erreichung des höchstmöglichen Resilienzwerts abgeschlossen werden müssen. Wenn diese Option ausgewählt ist, AWS Resilience Hub wird Folgendes angezeigt:
     - RTO/RPO— Gibt die Anzahl der Wiederherstellungszeiten (RTO/RPOs) an, die behoben werden müssen, um die Verstöße gegen die Ausfallsicherheitsrichtlinie Ihrer Anwendung zu beheben. Wählen Sie den Wert, um die RPO Details zuRTO/im Bewertungsbericht Ihrer Anwendung anzuzeigen.
     - Alarme — Gibt die Anzahl der empfohlenen CloudWatch Amazon-Alarme an, die in Ihrer Anwendung implementiert werden müssen. Wählen Sie den Wert aus, um die CloudWatch Amazon-Alarme anzuzeigen, die behoben werden müssen, im Bewertungsbericht Ihrer Anwendung.
     - SOPs— Gibt die Anzahl der Empfehlungen anSOPs, die in Ihrer Anwendung implementiert werden müssen. Wählen Sie den Wert aus, um SOPs die Werte anzuzeigen, die im Bewertungsbericht Ihrer Anwendung behoben werden müssen.
     - FIS— Gibt die Anzahl der empfohlenen Tests an, die in Ihrer Anwendung implementiert werden müssen. Wählen Sie den Wert aus, um die Tests anzuzeigen, die im Bewertungsbericht Ihrer Anwendung behoben werden müssen.
   - Um die Bewertung der einzelnen Komponenten anzuzeigen, die sich auf Ihre Resilienzbewertung auswirken, wählen Sie Aufschlüsselung der Ergebnisse aus. Wenn diese Option ausgewählt ist, AWS Resilience Hub wird Folgendes angezeigt:
     - RTO/RPOcompliance — Gibt an, wie konform die Anwendungskomponenten (AppComponents) mit den geschätzten Workload-Wiederherstellungszeiten und den Zielwiederherstellungszeiten sind, die in der Ausfallsicherheitsrichtlinie Ihrer Anwendung

definiert sind. Wählen Sie den Wert aus, um die RPO Schätzungen vonRTO/im Bewertungsbericht Ihrer Anwendung einzusehen.

- Implementierte Alarme — Zeigt den tatsächlichen Beitrag der implementierten CloudWatch Amazon-Alarme im Vergleich zu ihrem maximal möglichen Beitrag zum Stabilitätswert Ihrer Anwendung an. Wählen Sie den Wert aus, um die implementierten CloudWatch Amazon-Alarme im Bewertungsbericht Ihrer Anwendung anzuzeigen.
- SOPsimplementiert — Gibt den tatsächlichen Beitrag an, den die Implementierung SOPs im Vergleich zu ihrem maximal möglichen Beitrag zum Stabilitätswert Ihrer Anwendung geleistet hat. Wählen Sie den Wert aus, der SOPs im Bewertungsbericht Ihrer Anwendung angezeigt werden soll.
- FISimplementierte Experimente — Gibt den tatsächlichen Beitrag der implementierten Tests im Vergleich zu ihrem maximal möglichen Beitrag zum Stabilitätswert Ihrer Anwendung an. Wählen Sie den Wert aus, um die implementierten Tests im Bewertungsbericht Ihrer Anwendung anzuzeigen.

- Klicken Sie auf den Rechtspfeil, um den Abschnitt mit der Aufschlüsselung von Richtlinienverstößen und betrieblichen Empfehlungen zu öffnen, um die Verstöße gegen die Ausfallsicherheit und die betrieblichen Empfehlungen einzusehen. Im erweiterten Zustand wird AWS Resilience Hub Folgendes angezeigt:
  - Verstöße gegen die Ausfallsicherheitsrichtlinie — Gibt die Anzahl der Anwendungskomponenten an, die gegen die Ausfallsicherheitsrichtlinie Ihrer Anwendung verstoßen. Wählen Sie den Wert neben RTO/RPO, um die Details auf der Registerkarte Resilienzempfehlungen des Bewertungsberichts Ihrer Anwendung anzuzeigen.
  - Betriebsempfehlungen — Zeigt mithilfe der Registerkarten „Ausstehend“ und „Ausgeschlossen“ die Betriebsempfehlungen an, die nicht implementiert oder ausgeführt wurden, um die Ausfallsicherheit Ihrer Anwendung zu erhöhen. Zu den betrieblichen Empfehlungen gehören alle Empfehlungen, die inaktiv sind, und diejenigen, die nicht umgesetzt wurden.

    Um die operativen Empfehlungen anzuzeigen, die umgesetzt werden müssen, wählen Sie die Registerkarte Ausstehend. Wenn diese Option ausgewählt ist, AWS Resilience Hub wird Folgendes angezeigt:

    - Alarme — Gibt die Anzahl der empfohlenen CloudWatch Amazon-Alarme an, die implementiert werden müssen.
    - SOPs— Gibt die Anzahl der empfohlenen anSOPs, die implementiert werden müssen.
    - FIS— Gibt die Anzahl der empfohlenen Tests an, die implementiert werden müssen.

Um die Betriebsempfehlungen anzuzeigen, die aus Ihrer Anwendung ausgeschlossen sind, wählen Sie die Registerkarte Ausgeschlossen. Wenn diese Option ausgewählt ist, AWS Resilience Hub wird Folgendes angezeigt:

- Alarme — Gibt die Anzahl der empfohlenen CloudWatch Amazon-Alarme an, die von Ihrer Anwendung ausgeschlossen sind.
- SOPs— Gibt die Anzahl der empfohlenen anSOPs, die aus Ihrer Anwendung ausgeschlossen sind.
- FIS— Gibt die Anzahl der empfohlenen Tests an, die von Ihrer Anwendung ausgeschlossen sind.

Berechnung der Resilienzwerte

In den Tabellen in diesem Abschnitt werden die Formeln erläutert, mit AWS Resilience Hub denen die Bewertungskomponenten für die einzelnen Empfehlungstypen und die Resilienzbewertung Ihrer Anwendung bestimmt werden. Alle sich ergebenden Werte, die anhand AWS Resilience Hub der Bewertungskomponenten der einzelnen Empfehlungstypen und der Resilienzbewertung Ihrer Anwendung ermittelt wurden, werden auf den jeweils nächsten Punkt gerundet. Wenn beispielsweise zwei von drei Alarmen implementiert würden, läge die Punktzahl bei 13,33 (2/3) * 20) Punkten. Dieser Wert wird auf 13 Punkte gerundet. Weitere Informationen zu den Gewichten, die in den Formeln in den Tabellen verwendet werden, finden Sie im the section called “Gewichte AppComponents und Arten von Störungen” Abschnitt.

Einige der Bewertungskomponenten können nur über die abgerufen werden `ScoringComponentResiliencyScore`API. Weitere Informationen dazu finden Sie API unter ScoringComponentResiliencyScore.

Tabellen

- Formeln zur Berechnung der Bewertungskomponente der einzelnen Empfehlungstypen
- Formel zur Berechnung des Resilienz-Scores
- Formeln zur Berechnung der Resilienzbewertung AppComponents und der Störungstypen

In der folgenden Tabelle werden die Formeln erläutert AWS Resilience Hub , mit denen die Bewertungskomponente der einzelnen Empfehlungstypen berechnet wird.

Formeln zur Berechnung der Bewertungskomponente der einzelnen Empfehlungstypen

Bewertungskomponente	Beschreibung	Formel	Beispiel
Testabdeckung (T)	Eine normalisierte Punktzahl (0-100 Punkte), die auf der Anzahl der erfolgreich implementierten und ausgeschlossenen Tests von der Gesamtzahl der AWS Resilience Hub empfohlenen Tests basiert. **Note** Um den Resilienzwert zu berechnen, müssen die empfohlenen Tests in den letzten 30 Tagen erfolgreich ausgeführt worden sein, AWS Resilience Hub damit sie als implementiert betrachtet werden können.	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)` Teile der Formel lauten wie folgt: • Gesamtzahl der konfigurierten Tests — Gibt die Gesamtzahl der Tests an, die konfiguriert wurden, als die AWS CloudFormation Vorlage erstellt und in die AWS CloudFormation Konsole hochgeladen wurde. • Gesamtzahl der empfohlenen Tests — Gibt die Tests an, die von AWS Resilience Hub basierend auf den Anwendungsressourcen empfohlen wurden. • Gesamtzahl der ausgeschlossenen Tests — Gibt die Anzahl der empfohlenen Tests an, die Sie aus der	Wenn Sie 10 Tests implementiert und 5 von 20 AWS Resilience Hub empfohlenen Tests ausgeschlossen haben, wird die Testabdeckung wie folgt berechnet: `T = (10 + 5) / 20` Das heißt `T = .75 or 75 points`

Bewertung skomponente	Beschreibung	Formel	Beispiel
		Anwendung ausgeschl ossen haben.	

Bewertungskomponente	Beschreibung	Formel	Beispiel
Abdeckung von Alarmen (A)	Eine normalisierte Punktzahl (0-100 Punkte), die auf der Anzahl der CloudWatch Amazon-Alarme basiert, die erfolgreich implementiert und ausgeschlossen wurden, bezogen auf die Gesamtzahl der AWS Resilience Hub empfohlenen CloudWatch Amazon-Alarme. **Note** Um den Resilienzwert zu berechnen, sollten sich die empfohlenen Alarme im Status Bereit befinden, damit sie als AWS Resilience Hub implementiert gelten können.	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` Teile der Formel lauten wie folgt: • Gesamtzahl der konfigurierten Alarme — Gibt die Gesamtzahl der CloudWatch Amazon-Alarme an, die konfiguriert wurden, als die AWS CloudFormation Vorlage erstellt und in die AWS CloudFormation Konsole hochgeladen wurde. • Gesamtzahl der empfohlenen Alarme — Zeigt die von Amazon empfohlenen CloudWatch Alarme auf der AWS Resilience Hub Grundlage der Anwendungsressourcen an. • Gesamtzahl der ausgeschlossenen Alarme — Gibt die Anzahl der empfohlenen	Wenn Sie 10 von 20 AWS Resilience Hub empfohlenen CloudWatch Amazon-Alarmen implementiert und 5 ausgeschlossen haben, wird die CloudWatch Amazon-Alarmabdeckung wie folgt berechnet: CloudWatch `A = (10 + 5) / 20` Das heißt `A = .75 or 75 points`

Bewertung skomponente	Beschreibung	Formel	Beispiel
		CloudWatch Amazon-Al arme an, die Sie aus der Anwendung ausgeschl ossen haben.	

Bewertung skomponente	Beschreibung	Formel	Beispiel
SOPAbdeck ung (S)	Eine normalisierte Punktzahl (0-100 Punkte)SOPs, die auf der Anzahl der Empfehlun gen basiert, die erfolgreich umgesetzt und ausgeschl ossen wurden. AWS Resilience Hub SOPs	`S = ((Total number of SOPs implement ed) + (Total number of SOPs excluded) ) / (Total number of SOPs recommend ed)` Teile der Formel lauten wie folgt: • Gesamtzahl der SOPs konfigurierten — Gibt die Gesamtzahl der SOPs konfigurierten Dateien an, die beim Erstellen und Hochladen der AWS CloudFormation Vorlage in die AWS CloudForm ation Konsole konfiguri ert wurden. • Gesamtzahl der SOPs Empfehlun gen — Gibt die SOPs empfohlene Anzahl von AWS Resilience Hub basierend auf den Anwendungsressourcen an. • Gesamtzahl der SOPs ausgeschlossenen Personen — Gibt die Anzahl der empfohlenen Personen an, die SOPs	Wenn Sie 10 implementiert und 5 SOPs der AWS Resilience Hub empfohlenen 20 ausgeschlossen habenSOPs, wird der SOP Versicher ungsschutz wie folgt berechnet: `S = (10 + 5) / 20` Das heißt `S = .75 or 75 points`

Bewertung skomponente	Beschreibung	Formel	Beispiel
		Sie aus der Anwendung ausgeschlossen haben.	

Bewertungskomponente	Beschreibung	Formel	Beispiel
RTO/RPOEinhaltung (P)	Eine normalisierte Punktzahl (0-100 Punkte), die darauf basiert, dass die Anwendung ihre Stabilitätsrichtlinie erfüllt.	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	Wenn Ihre Richtlinie für die Ausfallsicherheit von Anwendungen nur für die Availability Zone (AZ) und die Art der Störung in der Infrastruktur erfüllt ist, wird die Bewertung der Ausfallsicherheitsrichtlinie (P) wie folgt berechnet: • Wenn Sie Regional RTO - und RPO Zielwerte festgelegt haben, P wird sie wie folgt berechnet: `P = (20 + 30)/ 100` Das heißt `P = .5 or 50 points` • Wenn Sie keine regionalen RPO Ziele RTO und Ziele festgelegt haben, P wird

Bewertung skomponente	Beschreibung	Formel	Beispiel
			dies wie folgt berechnet: `P = (22.22 + 33.33)/ 99.9` Das heißt `P = .55 or 55 points`

In der folgenden Tabelle wird die Formel erläutert AWS Resilience Hub , mit der der Resilienzwert für Ihre gesamte Anwendung berechnet wird.

Formel zur Berechnung des Resilienz-Scores

Bewertung skomponente	Beschreibung	Formel	Beispiel
Resilienz bewertung für die Anwendung () `RS`	Ein normalisierter Resilienz wert (0-100 Punkte), der darauf basiert, dass Ihre Anwendung ihre Stabilitätsrichtlinie erfüllt. Die Resilienzbewertung pro Anwendung ist der gewichtete Durchschnitt aller Empfehlungstypen. Das ist: `RS = Weighted Average (T, A, S, P)`	Die Resilienzbewertung pro Anwendung wird anhand der folgenden Formel berechnet: `RS = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))`	Die Formeln zur Berechnung des Umfangs der einzelnen Tabellen mit Empfehlun gstypen lauten wie folgt: • `Test coverage (T) = .75` • `Alarms (A) = .75` • `SOPs (S) = .75` • `Meeting resiliency`

Bewertung skomponente	Beschreibung	Formel	Beispiel

			`policy (P) = .5`
			
			Die Resilienz bewertung pro Anwendung wird wie folgt berechnet:
			
			`RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4)`
			
			Das heißt `RS = .65 or 65 points`

In der folgenden Tabelle werden die Formeln erläutert, die von AWS Resilience Hub zur Berechnung der Resilienzbewertung für Anwendungskomponenten (AppComponents) und Störungstypen verwendet werden. Sie können den Resilienzwert AppComponents und die Störungstypen jedoch nur über den folgenden AWS Resilience Hub abrufen: APIs

- DescribeAppAssessmentum zu erhalten `RSo`
- ListAppComponentComplianceszu erhalten `RSao` und `RSA`

Formeln zur Berechnung des Resilienzwerts AppComponents und der Störungsarten

Bewertungskomponente	Beschreibung	Formel	Beispiel

Resilienzbewertung pro AppComponent und pro Störungstyp () `RSao`	Ein normalisierter Wert (0-100 Punkte), der auf der AppComponent Einhaltung der Stabilitätsrichtlinien für jeden Störungstyp basiert. Der Resilienzwert pro AppComponent und pro Störungstyp ist der gewichtete Durchschnitt aller Empfehlungstypen.
	
	Das ist: `RSao = Weighted Average (T, A, S, P)`
	
	Die Werte für `T, A, S, P` werden für alle empfohlenen TestsSOPs, Alarme und
		Die Resilienzbewertung pro AppComponent und pro Störungstyp wird anhand der folgenden Formel berechnet:
		
		`RSao = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			`RSao`Die Annahmen für alle Empfehlungstypen lauten wie folgt:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			Der Resilienzwert pro AppComponent Störungsart wird wie folgt berechnet:
			
			`RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)`
			
			Das heißt `RSao = .65 or 65 points`

Bewertungskomponente	Beschreibung	Formel	Beispiel
	die Einhaltung der Ausfallsicherheitsrichtlinien für den Typ AppComponent und die Art der Störung berechnet.		

Bewertungskomponente	Beschreibung	Formel	Beispiel
Resilienzwert pro AppComponent () RSa	Ein normalisierter Wert (0-100 Punkte), der auf der Einhaltung der Stabilitätsrichtlinien basiert. Der Resilienzwert pro AppComponent ist der gewichtete Durchschnitt aller Empfehlungstypen. Das ist: RSa = Weighted Average (T, A, S, P) Die Werte für T, A, S, P werden für alle empfohlenen TestsSOPs, Alarme und die Einhaltung der AppComponent Stabilitätsrichtlinien von berechnet.	Der Resilienzwert pro AppComponent wird anhand der folgenden Formel berechnet: RSa = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	RSaDie Annahmen für alle Empfehlungstypen lauten wie folgt: • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 Der Resilienzwert pro AppComponent wird wie folgt berechnet: RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) Das heißt RSa = .65 or 65 points

Bewertungskomponente	Beschreibung	Formel	Beispiel

Resilienzbewertung pro Störungstyp () `RSo`	Ein normalisierter Wert (0-100 Punkte), der auf der Einhaltung der Stabilitätsrichtlinien basiert. Der Resilienzwert pro Störungstyp ist der gewichtete Durchschnitt aller Empfehlungstypen. Das ist: `RSo = Weighted Average (T, A, S, P)`
	
	Die Werte für `T, A, S, P` werden für alle empfohlenen TestsSOPs, Alarme und die Einhaltung der Ausfallsicherheitsrichtlinien für den jeweilige
		Die Resilienzbewertung pro Störungstyp wird anhand der folgenden Formel berechnet:
		
		`RSo = (T * Weight(T) + A * Weight(A) +`
		
		`S * Weight(S) + P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			`RSo`Die Annahmen für alle Empfehlungstypen lauten wie folgt:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			Die Resilienzbewertung pro Störungstyp wird wie folgt berechnet:
			
			`RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) /`
			
			`(.2 + .2 + .2 + .4)`
			
			Das heißt `RSo = .65 or 65 points`

Bewertung skomponente	Beschreibung	Formel	Beispiel
	n Störungstyp berechnet.		

Gewichte

AWS Resilience Hub weist jedem Empfehlungstyp eine Gewichtung für den Gesamtwert der Ausfallsicherheit zu.

In den folgenden Tabellen wird die Gewichtung für Alarme, TestsSOPs, Einhaltung der Stabilitätsrichtlinien und Störungsarten dargestellt. Zu den Störungstypen gehören Anwendung, Infrastruktur, AZ und Region.

> **Note**
>
> Wenn Sie sich dafür entscheiden, für Ihre Police keine Region RTO oder RPO Zielvorgaben zu definieren, werden die Gewichtungen für die anderen Störungsarten entsprechend erhöht, wie in der Spalte Gewichtung, wenn Region nicht definiert ist, angegeben.

Gewichte für AlarmeSOPs, Tests und politisches Ziel

Art der Empfehlung	Gewicht
Alarme	20 Punkte
SOPs	20 Punkte
Tests	20 Punkte
Einhaltung der Resilienzpolitik	40 Punkte

Gewichte für die Art der Störung

Art der Störung	Gewicht, wenn Region definiert ist	Gewicht, wenn Region nicht definiert ist
Anwendung	40 Punkte	44,44 Punkte
Infrastruktur	30 Punkte	33,33 Punkte
Availability Zone	20 Punkte	22,22 Punkte
Region	10 Punkte	N/A

Integrieren von Betriebsempfehlungen in Ihre Anwendung mit AWS CloudFormation

Nachdem Sie auf der Seite Betriebsempfehlungen die Option CloudFormation Vorlage erstellen ausgewählt haben, AWS Resilience Hub wird eine AWS CloudFormation Vorlage erstellt, die den spezifischen Alarm, die Standardarbeitsanweisung (SOP) oder das AWS FIS Experiment für Ihre Anwendung beschreibt. Die AWS CloudFormation Vorlage wird in einem Amazon S3 S3-Bucket gespeichert, und Sie können den S3-Pfad zur Vorlage auf der Registerkarte Vorlagendetails auf der Seite Betriebsempfehlungen überprüfen.

Die folgende Liste zeigt beispielsweise eine AWS CloudFormation Vorlage im JSON -Format, die eine Alarmempfehlung beschreibt, die von ausgegeben wurde. AWS Resilience Hub Es ist ein Read Throttling Alarm für eine DynamoDB-Tabelle namens. `Employees`

Der `Resources` Abschnitt der Vorlage beschreibt den `AWS::CloudWatch::Alarm` Alarm, der aktiviert wird, wenn die Anzahl der Read-Throttle-Ereignisse für die DynamoDB-Tabelle 1 überschreitet. Und die beiden `AWS::SSM::Parameter` Ressourcen definieren Metadaten, die es ermöglichen, installierte Ressourcen AWS Resilience Hub zu identifizieren, ohne die eigentliche Anwendung scannen zu müssen.

```
{
  "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."
      }
    }
  }
}
```

Änderung der AWS CloudFormation Vorlage

Der einfachste WegSOP, einen Alarm oder eine AWS FIS Ressource in Ihre Hauptanwendung zu integrieren, besteht darin, sie einfach als weitere Ressource zu der Vorlage hinzuzufügen, die Ihre Anwendungsvorlage beschreibt. Die unten bereitgestellte JSON Datei im -Format bietet einen grundlegenden Überblick darüber, wie eine DynamoDB-Tabelle in einer Vorlage beschrieben wird.

AWS CloudFormation Eine echte Anwendung enthält wahrscheinlich mehrere weitere Ressourcen, z. B. zusätzliche Tabellen.

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

Damit die Alarm-Ressource zusammen mit Ihrer Anwendung bereitgestellt werden kann, müssen Sie jetzt die fest codierten Ressourcen durch eine dynamische Referenz in den Anwendungsstapeln ersetzen.

Ändern Sie also in der `AWS::CloudWatch::Alarm` Ressourcendefinition Folgendes:

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

zum Folgenden:

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

Und ändern Sie in der `AWS::SSM::Parameter` Ressourcendefinition Folgendes:

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

zum Folgenden:

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

Beim Ändern von AWS CloudFormation Vorlagen für SOPs und AWS FIS Experimente verwenden Sie denselben Ansatz und ersetzen hartcodierte Verweise IDs durch dynamische Verweise, die auch nach Hardwareänderungen weiterhin funktionieren.

Durch die Verwendung eines Verweises auf die DynamoDB-Tabelle AWS CloudFormation ermöglichen Sie Folgendes:

- Erstellen Sie zuerst die Datenbanktabelle.
- Verwenden Sie immer die tatsächliche ID der generierten Ressource im Alarm und aktualisieren Sie den Alarm dynamisch, falls die Ressource ersetzt AWS CloudFormation werden muss.

> **Note**
>
> Sie können erweiterte Methoden für die Verwaltung Ihrer Anwendungsressourcen wählen, AWS CloudFormation z. B. indem Sie Stacks verschachteln oder auf

Ressourcenausgaben in einem separaten AWS CloudFormation Stapel verweisen. (Wenn Sie den Empfehlungsstapel jedoch vom Hauptstapel trennen möchten, müssen Sie eine Methode für die Informationsübertragung zwischen den beiden Stacks konfigurieren.) Darüber hinaus können Tools von Drittanbietern wie Terraform by HashiCorp auch zur Bereitstellung von Infrastructure as Code (IaC) verwendet werden.

Wird AWS Resilience Hub APIs zur Beschreibung und Verwaltung der Anwendung verwendet

Als Alternative zur Beschreibung und Verwaltung von Anwendungen mithilfe der AWS Resilience Hub Konsole AWS Resilience Hub ermöglicht es Ihnen, Anwendungen mithilfe von zu beschreiben und zu verwalten AWS Resilience Hub APIs. In diesem Kapitel wird erklärt, wie Sie eine Anwendung mithilfe von erstellen AWS Resilience Hub APIs. Es definiert auch die Reihenfolge, in der Sie die ausführen müssen, APIs und die Parameterwerte, die Sie mit entsprechenden Beispielen angeben müssen. Weitere Informationen finden Sie unter den folgenden Themen:

- the section called “Vorbereitung des Antrags”
- the section called “Ausführung und Analyse der Anwendung”
- the section called “Ändern Sie Ihre Bewerbung”

Schritt 1: Vorbereitung der Anwendung

Um eine Anwendung vorzubereiten, müssen Sie zuerst eine Anwendung erstellen, eine Ausfallsicherheitsrichtlinie zuweisen und dann die Anwendungsressourcen aus Ihren Eingabequellen importieren. Weitere Informationen zu den AWS Resilience Hub APIs, die zur Vorbereitung einer Anwendung verwendet werden, finden Sie in den folgenden Themen:

- the section called “Erstellen einer Anwendung”
- the section called “Erstellen Sie eine Resilienzrichtlinie”
- the section called “Importieren Sie die Anwendungsressource und überwachen Sie den Importstatus”
- the section called “Veröffentlichen Sie Ihre Anwendung und weisen Sie ihnen eine Ausfallsicherheitsrichtlinie zu”

Erstellen einer Anwendung

Um eine neue Anwendung in zu erstellen AWS Resilience Hub, müssen Sie die aufrufen `CreateApp` API und einen eindeutigen Anwendungsnamen angeben. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

Das folgende Beispiel zeigt, wie Sie eine neue Anwendung `newApp` in AWS Resilience Hub Using erstellen `CreateApp`API.

Anforderung

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

Antwort

```
{
    "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"
    }
}
```

Erstellung einer Resilienzrichtlinie

Nachdem Sie die Anwendung erstellt haben, müssen Sie eine Ausfallsicherheitsrichtlinie erstellen, anhand derer Sie den Ausfallsicherheitsstatus Ihrer Anwendung nachvollziehen können. `CreateResiliencyPolicy` API Weitere Informationen dazu API finden Sie unter. https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html

Das folgende Beispiel zeigt, wie Sie `newPolicy` für Ihre Anwendung erstellen `CreateResiliencyPolicy`API. AWS Resilience Hub

Anforderung

```
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}}'
```

Antwort

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

Ressourcen aus einer Eingabequelle importieren und den Importstatus überwachen

AWS Resilience Hub bietet FolgendesAPIs, um Ressourcen in Ihre Anwendung zu importieren:

- `ImportResourcesToDraftAppVersion`— API Auf diese Weise können Sie Ressourcen aus verschiedenen Eingabequellen in die Entwurfsversion Ihrer Anwendung importieren. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- `PublishAppVersion`— Dadurch wird eine neue Version der Anwendung zusammen mit der aktualisierten Version API veröffentlicht AppComponents. Weitere Informationen dazu

finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

- `DescribeDraftAppVersionResourcesImportStatus`— API Auf diese Weise können Sie den Importstatus Ihrer Ressourcen in eine Anwendungsversion überwachen. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

Das folgende Beispiel zeigt, wie Sie Ressourcen in Ihre Anwendung importieren, die Sie AWS Resilience Hub verwenden `ImportResourcesToDraftAppVersion`API.

Anforderung

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

Antwort

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

Das folgende Beispiel zeigt, wie Sie Ihrer Anwendung manuell Ressourcen hinzufügen können, die gerade AWS Resilience Hub verwendet `CreateAppVersionResource` API werden.

Anforderung

```
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"]'
```

Antwort

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

Das folgende Beispiel zeigt, wie Sie den Importstatus Ihrer AWS Resilience Hub verwendeten Ressourcen überwachen können `DescribeDraftAppVersionResourcesImportStatus`API.

Anforderung

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

Antwort

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

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

Veröffentlichung der Entwurfsversion Ihrer Anwendung und Zuweisung einer Ausfallsicherheitsrichtlinie

Bevor Sie eine Bewertung durchführen, müssen Sie zunächst die Entwurfsversion Ihrer Anwendung veröffentlichen und der veröffentlichten Version Ihrer Anwendung eine Ausfallsicherheitsrichtlinie zuweisen.

Um die Entwurfsversion Ihrer Anwendung zu veröffentlichen und eine Ausfallsicherheitsrichtlinie zuzuweisen

1. Um die Entwurfsversion Ihrer Anwendung zu veröffentlichen, verwenden Sie `PublishAppVersion`API. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

   Das folgende Beispiel zeigt, wie die Entwurfsversion der Anwendung veröffentlicht wird, die gerade AWS Resilience Hub verwendet wird `PublishAppVersion`API.

   Anforderung

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

   Antwort

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

2. Wenden Sie eine Ausfallsicherheitsrichtlinie auf die veröffentlichte Version Ihrer Anwendung an, indem `UpdateApp` API Sie. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html.

Das folgende Beispiel zeigt, wie eine Resilienzrichtlinie auf die veröffentlichte Version einer Anwendung angewendet wird, die gerade AWS Resilience Hub verwendet `UpdateApp` API wird.

Anforderung

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

Antwort

```
{
    "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"
    }
}
```

Schritt 2: Durchführung und Verwaltung von AWS Resilience Hub Resilienzbewertungen

Nachdem Sie eine neue Version Ihrer Anwendung veröffentlicht haben, müssen Sie eine neue Resilienzbewertung durchführen und die Ergebnisse analysieren, um sicherzustellen, dass Ihre Anwendung die geschätzte RTO und geschätzte Arbeitslast erfülltRPO, die in Ihrer Resilienzrichtlinie definiert sind. Bei der Bewertung wird jede Konfiguration der Anwendungskomponente mit der Richtlinie verglichen und es werden Alarm- und SOP Testempfehlungen ausgesprochen.

Weitere Informationen finden Sie unter den folgenden Themen:

- the section called “Führen Sie eine Resilienzbewertung durch und überwachen Sie sie”
- the section called “Erstellen Sie eine Resilienzrichtlinie”

Durchführung und Überwachung von AWS Resilience Hub Resilienzbewertungen

Um Resilienzbewertungen durchzuführen AWS Resilience Hub und deren Status zu überwachen, müssen Sie Folgendes verwenden: APIs

- `StartAppAssessment`— API Dadurch wird eine neue Bewertung für eine Anwendung erstellt. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.
- `DescribeAppAssessment`— Darin API wird eine Bewertung für den Antrag beschrieben und der Abschlussstatus der Prüfung angegeben. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

Das folgende Beispiel zeigt, wie Sie mit der Ausführung einer neuen Bewertung in der AWS Resilience Hub Anwendung beginnen `StartAppAssessment`API.

Anforderung

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

Antwort

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

Das folgende Beispiel zeigt, wie Sie den Status Ihrer Bewertung im AWS Resilience Hub Einsatz überwachen können `DescribeAppAssessment`API. Sie können den Status Ihrer Bewertung aus der `assessmentStatus` Variablen extrahieren.

Anforderung

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

Antwort

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

Prüfung der Bewertungsergebnisse

Nachdem Ihre Bewertung erfolgreich abgeschlossen wurde, können Sie die Prüfungsergebnisse anhand der folgenden Methoden überprüfenAPIs.

- `DescribeAppAssessment`— API Auf diese Weise können Sie den aktuellen Status Ihrer Anwendung anhand der Resilienz-Richtlinie verfolgen. Darüber hinaus können Sie auch den Compliance-Status aus einer `complianceStatus` Variablen und die Resilienzbewertung für jeden Störungstyp aus der `resiliencyScore` Struktur extrahieren. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.
- `ListAlarmRecommendations`— API Auf diese Weise können Sie die Alarmempfehlungen mithilfe des Amazon-Ressourcennamens (ARN) der Bewertung abrufen. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html.

> **Note**
>
> Verwenden Sie SOP und, um die Empfehlungen zu erhalten `ListSopRecommendations` und zu FIS testen `ListTestRecommendations`APIs.

Das folgende Beispiel zeigt, wie Sie die Alarmempfehlungen mithilfe des Amazon-Ressourcennamens (ARN) der Bewertung mithilfe von abrufen können `ListAlarmRecommendations`API.

> **Note**
>
> Um die Empfehlungen zu erhalten SOP und zu FIS testen, ersetzen Sie sie durch entweder `ListSopRecommendations` oder`ListTestRecommendations`.

Anforderung

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

Antwort

```
{
    "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>)."
        }
    ]
}
```

Das folgende Beispiel zeigt, wie Sie die Konfigurationsempfehlungen (Empfehlungen zur Verbesserung Ihrer aktuellen Resilienz) mithilfe von `ListAppComponentRecommendations` API erhalten.

Anforderung

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

Antwort

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

Schritt 3: Ändern Ihrer Anwendung

AWS Resilience Hub ermöglicht es Ihnen, Ihre Anwendungsressourcen zu ändern, indem Sie eine Entwurfsversion Ihrer Anwendung bearbeiten und die Änderungen in einer neuen (veröffentlichten) Version veröffentlichen. AWS Resilience Hub verwendet die veröffentlichte Version Ihrer Anwendung, die die aktualisierten Ressourcen enthält, für die Durchführung von Resilienzbewertungen.

Weitere Informationen finden Sie unter den folgenden Themen:

- the section called “Manuelles Hinzufügen von Ressourcen”
- the section called “Gruppierung von Ressourcen in einer einzigen Anwendungskomponente”
- the section called “Ausschließen einer Ressource aus einem AppComponent”

Manuelles Hinzufügen von Ressourcen zu Ihrer Anwendung

Wenn die Ressource nicht als Teil einer Eingabequelle bereitgestellt wird, AWS Resilience Hub können Sie die Ressource mithilfe von manuell zu Ihrer Anwendung hinzufügen `CreateAppVersionResource`API. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

Dazu müssen Sie die folgenden Parameter angebenAPI:

- Amazon-Ressourcenname (ARN) der Anwendung
- Logische ID der Ressource
- Physikalische ID der Ressource
- AWS CloudFormation Typ

Das folgende Beispiel zeigt, wie Sie Ihrer Anwendung manuell Ressourcen hinzufügen, die gerade AWS Resilience Hub verwendet `CreateAppVersionResource` API werden.

Anforderung

```
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"]'
```

Antwort

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

Gruppieren von Ressourcen in einer einzigen Anwendungskomponente

Eine Anwendungskomponente (AppComponent) ist eine Gruppe verwandter AWS Ressourcen, die als eine Einheit funktionieren und ausfallen. Dies ist beispielsweise der Fall, wenn Sie über regionsübergreifende Workloads verfügen, die als Standby-Bereitstellungen verwendet werden. AWS Resilience Hub enthält Regeln, die festlegen, welche AWS Ressourcen zu welchem Typ gehören

können. AppComponent AWS Resilience Hub ermöglicht es Ihnen, Ressourcen AppComponent mithilfe der folgenden Ressourcenverwaltung zu einer einzigen zusammenzufassenAPIs.

- `UpdateAppVersionResource`— Dadurch werden die Ressourcendetails einer Anwendung API aktualisiert. Weitere Informationen dazu finden Sie API unter UpdateAppVersionResource.
- `DeleteAppVersionAppComponent`— Dadurch wird das AppComponent aus der Anwendung API gelöscht. Weitere Informationen dazu finden Sie API unter DeleteAppVersionAppComponent.

Das folgende Beispiel zeigt, wie Sie die Ressourcendetails Ihrer Anwendung aktualisieren, die gerade AWS Resilience Hub verwendet wird `DeleteAppVersionAppComponent`API.

Anforderung

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

Antwort

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

Das folgende Beispiel zeigt, wie Sie die leere Datei löschen AppComponent , die in den vorherigen Anwendungsbeispielen erstellt wurde `UpdateAppVersionResource`API. AWS Resilience Hub

Anforderung

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

Antwort

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

Ausschließen einer Ressource aus einem AppComponent

AWS Resilience Hub ermöglicht es Ihnen, Ressourcen von Bewertungen auszuschließen mithilfe von `UpdateAppVersionResource`API. Diese Ressourcen werden bei der Berechnung der Ausfallsicherheit Ihrer Anwendung nicht berücksichtigt. Weitere Informationen dazu finden Sie API unterhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html.

> **Note**
>
> Sie können nur die Ressourcen ausschließen, die aus einer Eingabequelle importiert wurden.

Das folgende Beispiel zeigt, wie Sie eine Ressource ausschließen, die von Ihrer Anwendung AWS Resilience Hub verwendet wird `UpdateAppVersionResource`API.

Anforderung

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

Antwort

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

Sicherheit in AWS Resilience Hub

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Resilience Hub, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS Resilience Hub. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Resilience Hub , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Resilience Hub Ressourcen unterstützen.

Inhalt

Datenschutz in AWS Resilience Hub

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Resilience Hub. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten.

Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS -Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag im AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS -Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard () 140-3. FIPS

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Resilience Hub oder anderen Geräten AWS -Services über die Konsole,API, AWS CLI oder arbeiten. AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

Verschlüsselung im Ruhezustand

AWS Resilience Hub verschlüsselt Ihre Daten im Ruhezustand. Eingeschlossene Daten werden im AWS Resilience Hub Ruhezustand mit transparenter serverseitiger Verschlüsselung verschlüsselt. Dieser Service reduziert den Ausführungsaufwand und die Komplexität, die mit dem Schutz

sensibler Daten verbunden sind. Mit der Verschlüsselung von Daten im Ruhezustand können Sie sicherheitsrelevante Anwendungen erstellen, die Verschlüsselungsvorschriften und gesetzliche Bestimmungen einhalten.

Verschlüsselung während der Übertragung

AWS Resilience Hub verschlüsselt Daten, die zwischen dem Dienst und anderen integrierten AWS Diensten übertragen werden. Alle Daten, die zwischen AWS Resilience Hub und integrierten Diensten übertragen werden, werden mit Transport Layer Security (TLS) verschlüsselt. AWS Resilience Hub stellt AWS dienstübergreifend vorkonfigurierte Aktionen für bestimmte Zieltypen bereit und unterstützt Aktionen für Zielressourcen.

Identity and Access Management für AWS Resilience Hub

AWS Identity and Access Management (IAM) hilft einem Administrator AWS -Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um AWS Resilience Hub-Ressourcen zu nutzen. IAMist eine AWS -Service , die Sie ohne zusätzliche Kosten nutzen können.

Themen

- Beschränken Sie die Berechtigungen auf das Ein- oder Ausschließen von AWS Resilience Hub Empfehlungen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in AWS Resilience Hub ausführen.

Dienstbenutzer — Wenn Sie den AWS Resilience Hub-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Wenn Sie für Ihre Arbeit mehr AWS Resilience Hub-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Funktion in AWS Resilience Hub nicht zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Identität und Zugriff auf AWS Resilience Hub.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für AWS Resilience Hub-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS Resilience Hub. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Resilience Hub-Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen AWS Resilience Hub nutzen IAM kann, finden Sie unterWie funktioniert AWS Resilience Hub mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf AWS Resilience Hub zu verwalten. Beispiele für identitätsbasierte AWS Resilience Hub-Richtlinien, die Sie verwenden könnenIAM, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Resilience Hub

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-

Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS -Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS -Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS -Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS -Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS -Services verwenden Funktionen in anderen. AWS -Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS -Service, kombiniert mit der Anforderung, Anfragen AWS -Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS -Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS -Service an eine.
- Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS -Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den

Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und

Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS -Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung

mehrerer Geräte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie funktioniert AWS Resilience Hub mit IAM

Bevor Sie IAM den Zugriff auf AWS Resilience Hub verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen für AWS Resilience Hub verfügbar sind.

IAMFunktionen, die Sie mit AWS Resilience Hub verwenden können

IAMFunktion	AWS Resilience Hub-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja

IAMFunktion	AWS Resilience Hub-Unterstützung
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC(Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Zugriffssitzungen weiterleiten (FAS)	Ja
Servicerollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Resilience Hub und andere AWS Dienste mit den meisten IAM Funktionen funktionieren, finden Sie IAM im IAMBenutzerhandbuch unter AWS Dienste, die mit funktionieren.

Identitätsbasierte Richtlinien für AWS Resilience Hub

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Resilience Hub

Beispiele für identitätsbasierte Richtlinien von AWS Resilience Hub finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Resilience Hub

Ressourcenbasierte Richtlinien innerhalb von Resilience Hub AWS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie einer Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS -Services

Um den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie IAMim IAMBenutzerhandbuch unter Kontenübergreifender Ressourcenzugriff.

Politische Maßnahmen für AWS Resilience Hub

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt.

API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS Resilience Hub-Aktionen finden Sie unter Von AWS Resilience Hub definierte Aktionen in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen in AWS Resilience Hub wird vor der Aktion das folgende Präfix verwendet:

```
resiliencehub
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für identitätsbasierte Richtlinien von AWS Resilience Hub finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Resilience Hub

Politische Ressourcen für Resilience Hub AWS

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AWS Resilience Hub-Ressourcentypen und ihrer Eigenschaften ARNs finden Sie unter Von AWS Resilience Hub definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter Von AWS Resilience Hub definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von AWS Resilience Hub finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Resilience Hub

Schlüssel zu den Bedingungen der Richtlinien für Resilience Hub AWS

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

Eine Liste der AWS Resilience Hub-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Resilience Hub in der Serviceautorisierungsreferenz. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Resilience Hub definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von AWS Resilience Hub finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Resilience Hub

ACLsim AWS Resilience Hub

UnterstütztACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABACmit AWS Resilience Hub

Unterstützungen ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt vonABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Verwendung temporärer Anmeldeinformationen mit Resilience Hub AWS

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS -Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS -Services wie Sie mit temporären Anmeldeinformationen arbeiten können AWS -Services , finden Sie IAM im IAMBenutzerhandbuch unter Informationen zum Arbeiten mit.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAMBenutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen unter IAM.

Zugriffssitzungen für AWS Resilience Hub weiterleiten

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS -Service, kombiniert mit der Anforderung, Anfragen AWS -Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS -Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Resilience Hub

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS -Service an eine.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS Resilience Hub-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn AWS Resilience Hub Sie dazu anleitet.

Beispiele für identitätsbasierte Richtlinien für AWS Resilience Hub

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS Resilience Hub-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen AWS API. Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

Einzelheiten zu den von AWS Resilience Hub definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resilience Hub in der Referenz zur Serviceautorisierung.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS Resilience Hub-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Verfügbare Anwendungen auflisten AWS Resilience Hub

- Starten einer Anwendungsbewertung
- Löschen einer Anwendungsbewertung
- Erstellen einer Empfehlungsvorlage für eine bestimmte Anwendung
- Löschen einer Empfehlungsvorlage für eine bestimmte Anwendung
- Aktualisierung einer Anwendung mit einer bestimmten Ausfallsicherheitsrichtlinie

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Resilience Hub-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS -Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende

Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.

- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwenden der AWS Resilience Hub-Konsole

Um auf die AWS Resilience Hub-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Resilience Hub-Ressourcen in Ihrem aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur Anrufe an den AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS Resilience Hub-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch den AWS Resilience Hub *ConsoleAccess* oder die *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer.

Die folgende Richtlinie gewährt Benutzern die Berechtigung, alle Ressourcen in der AWS Resilience Hub Konsole aufzulisten und anzuzeigen, sie jedoch nicht zu erstellen, zu aktualisieren oder zu löschen.

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

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

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die internen und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
```

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Verfügbare Anwendungen auflisten AWS Resilience Hub

Die folgende Richtlinie gewährt Benutzern die Berechtigung, die verfügbaren AWS Resilience Hub Anwendungen aufzulisten.

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

Starten einer Anwendungsbewertung

Die folgende Richtlinie gewährt Benutzern die Erlaubnis, eine Bewertung für eine bestimmte AWS Resilience Hub Anwendung zu starten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:StartAppAssessment"
      ],
```

```
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Löschen einer Anwendungsbewertung

Die folgende Richtlinie gewährt Benutzern die Berechtigung, eine Bewertung für eine bestimmte AWS Resilience Hub Anwendung zu löschen.

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

Erstellen einer Empfehlungsvorlage für eine bestimmte Anwendung

Die folgende Richtlinie gewährt Benutzern die Berechtigung, eine Empfehlungsvorlage für eine bestimmte AWS Resilience Hub Anwendung zu erstellen.

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

```
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Löschen einer Empfehlungsvorlage für eine bestimmte Anwendung

Die folgende Richtlinie gewährt Benutzern die Berechtigung, eine Empfehlungsvorlage für eine bestimmte AWS Resilience Hub Anwendung zu löschen.

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

Aktualisierung einer Anwendung mit einer bestimmten Ausfallsicherheitsrichtlinie

Die folgende Richtlinie gewährt Benutzern die Berechtigung, eine AWS Resilience Hub Anwendung mit einer bestimmten Ausfallsicherheitsrichtlinie zu aktualisieren.

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

```
      ],
      "Condition": {
        "StringLike" : { "resiliencehub:policyArn" : "arn:aws:resiliencehub:us-
west-2:111122223333:resiliency-policy/*" }
      }
    }
  ]
}
```

IAMRollen und Berechtigungen einrichten

AWS Resilience Hub ermöglicht es Ihnen, die IAM Rollen zu konfigurieren, die Sie bei der Durchführung von Assessments für Ihre Anwendung verwenden möchten. Es gibt mehrere Möglichkeiten zur Konfiguration, AWS Resilience Hub um nur Lesezugriff auf Ihre Anwendungsressourcen zu erhalten. AWS Resilience Hub Empfiehlt jedoch die folgenden Methoden:

- Rollenbasierter Zugriff — Diese Rolle wird im aktuellen Konto definiert und verwendet. AWS Resilience Hub übernimmt diese Rolle, um auf die Ressourcen Ihrer Anwendung zuzugreifen.

  Um den rollenbasierten Zugriff zu ermöglichen, muss die Rolle Folgendes beinhalten:

  - Schreibgeschützte Berechtigung zum Lesen Ihrer Ressourcen (AWS Resilience Hub empfiehlt die Verwendung der `AWSResilienceHubAsssessmentExecutionPolicy` verwalteten Richtlinie).
  - Vertrauen Sie darauf, dass die Richtlinie diese Rolle übernimmt, sodass AWS Resilience Hub Service Principal diese Rolle übernehmen kann. Wenn Sie eine solche Rolle in Ihrem Konto nicht konfiguriert haben, AWS Resilience Hub werden die Anweisungen zum Erstellen dieser Rolle angezeigt. Weitere Informationen finden Sie unter the section called “Schritt 6: Berechtigungen einrichten”.

  > **Note**
  >
  > Wenn Sie nur den Namen der Aufruferrolle angeben und wenn sich Ihre Ressourcen in einem anderen Konto befinden, AWS Resilience Hub wird dieser Rollenname in den anderen Konten verwendet, um auf die kontoübergreifenden Ressourcen zuzugreifen. Optional können Sie die Rolle ARNs für andere Konten konfigurieren, die anstelle des Rollennamens des Aufrufers verwendet werden.

- Aktueller IAM Benutzerzugriff — verwendet AWS Resilience Hub den aktuellen IAM Benutzer für den Zugriff auf Ihre Anwendungsressourcen. Wenn sich Ihre Ressourcen in einem anderen Konto

befinden, AWS Resilience Hub übernimmt er beim Zugriff auf die Ressourcen die folgenden IAM Rollen:

- `AwsResilienceHubAdminAccountRole`auf dem Girokonto
- `AwsResilienceHubExecutorAccountRole`auf anderen Konten

Darüber hinaus übernimmt er die `AwsResilienceHubPeriodicAssessmentRole` Rolle, AWS Resilience Hub wenn Sie eine geplante Bewertung konfigurieren. Von der Verwendung `AwsResilienceHubPeriodicAssessmentRole` wird jedoch abgeraten, da Sie Rollen und Berechtigungen manuell konfigurieren müssen und einige Funktionen (z. B. Drift-Benachrichtigungen) möglicherweise nicht wie erwartet funktionieren.

Fehlerbehebung bei Identität und Zugriff auf AWS Resilience Hub

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Resilience Hub und auftreten könnenIAM.

Themen

- Ich bin nicht berechtigt, eine Aktion in AWS Resilience Hub durchzuführen
- Ich bin nicht berechtigt, iam durchzuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Resilience Hub-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in AWS Resilience Hub durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven `resiliencehub:`*`GetWidget`* Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `resiliencehub:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Durchführung der `iam:PassRole` Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an AWS Resilience Hub übergeben können.

Einige AWS -Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Resilience Hub auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Resilience Hub-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob AWS Resilience Hub diese Funktionen unterstützt, finden Sie unter. Wie funktioniert AWS Resilience Hub mit IAM

- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM Benutzerhandbuch unter Gewähren des Zugriffs auf einen anderen IAMBenutzer AWS-Konto , der Ihnen gehört.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

AWS Resilience Hub Referenz zu Zugriffsberechtigungen

Sie können AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf die Anwendungsressourcen zu verwalten und IAM Richtlinien zu erstellen, die für Benutzer, Gruppen oder Rollen gelten.

Jede AWS Resilience Hub Anwendung kann so konfiguriert werden, dass sie die the section called “Rolle des Aufrufers” (eine IAM Rolle) oder die aktuellen IAM Benutzerberechtigungen (zusammen mit einer Reihe vordefinierter Rollen für kontoübergreifende und geplante Bewertungen) verwendet. In dieser Rolle können Sie eine Richtlinie anfügen, die die Berechtigungen definiert, die für den AWS Resilience Hub Zugriff auf andere AWS Ressourcen oder Anwendungsressourcen erforderlich sind. Die Aufruferrolle muss über eine Vertrauensrichtlinie verfügen, die dem AWS Resilience Hub Service Principal hinzugefügt wird.

Um die Berechtigungen für Ihre Anwendung zu verwalten, empfehlen wir die Verwendung vonthe section called “AWS verwaltete Richtlinien”. Sie können diese verwalteten Richtlinien ohne Änderungen verwenden, oder Sie können sie als Ausgangspunkt verwenden, um Ihre eigenen restriktiven Richtlinien zu schreiben. Richtlinien können Benutzerberechtigungen auf Ressourcenebene für verschiedene Aktionen einschränken, indem zusätzliche optionale Bedingungen verwendet werden.

Wenn sich Ihre Anwendungsressourcen in unterschiedlichen Konten befinden (Sekundärkonten oder Ressourcenkonten), müssen Sie für jedes Konto, das Ihre Anwendungsressourcen enthält, eine neue Rolle einrichten.

Topics

- the section called “IAMRolle wird verwendet”
- the section called “Aktuelle IAM Benutzerberechtigungen verwenden”

Rolle verwenden IAM

AWS Resilience Hub verwendet eine vordefinierte vorhandene IAM Rolle, um auf Ihre Ressourcen im primären Konto oder im sekundären Konto bzw. im Ressourcenkonto zuzugreifen. Dies ist die empfohlene Berechtigungsoption für den Zugriff auf Ihre Ressourcen.

Topics

- the section called “Rolle des Aufrufers”
- the section called “Rollen in verschiedenen AWS Konten für kontoübergreifenden Zugriff”

Rolle des Aufrufers

Die AWS Resilience Hub Aufruferrolle ist eine AWS Identity and Access Management (IAM) -Rolle, die AWS Resilience Hub davon ausgeht, auf AWS Dienste und Ressourcen zuzugreifen. Sie könnten beispielsweise eine Aufruferrolle erstellen, die berechtigt ist, auf Ihre CFN Vorlage und die von ihr erstellte Ressource zuzugreifen. Diese Seite enthält Informationen zum Erstellen, Anzeigen und Verwalten einer Anwendungsaufruferrolle.

Wenn Sie eine Anwendung erstellen, geben Sie eine Aufruferrolle an. AWS Resilience Hub nimmt diese Rolle für den Zugriff auf Ihre Ressourcen an, wenn Sie Ressourcen importieren oder eine Bewertung starten. AWS Resilience Hub Damit Sie Ihre Rolle als Aufrufer ordnungsgemäß wahrnehmen können, muss in der Vertrauensrichtlinie der Rolle der AWS Resilience Hub Service Principal (resiliencehub.amazonaws.com) als vertrauenswürdiger Service angegeben sein.

Um die Aufruferrolle der Anwendung anzuzeigen, wählen Sie im Navigationsbereich Anwendungen und dann auf der Anwendungsseite im Menü Aktionen die Option Berechtigungen aktualisieren aus.

Sie können einer Anwendungsaufruferrolle jederzeit Berechtigungen hinzufügen oder daraus entfernen oder Ihre Anwendung so konfigurieren, dass sie eine andere Rolle für den Zugriff auf Anwendungsressourcen verwendet.

Topics

- the section called “Eine Aufruferrolle in der Konsole erstellen IAM”

- the section called “Rollen verwalten mit dem IAM API”
- the section called “Definition einer Vertrauensrichtlinie mithilfe einer JSON Datei”

Eine Aufruferrolle in der Konsole erstellen IAM

Um den Zugriff auf AWS Dienste und Ressourcen AWS Resilience Hub zu ermöglichen, müssen Sie mithilfe der Konsole eine Aufruferrolle im primären Konto erstellen. IAM Weitere Informationen zum Erstellen von Rollen mithilfe der IAM Konsole finden Sie unter Erstellen einer Rolle für einen AWS Dienst (Konsole).

So erstellen Sie mithilfe IAM der Konsole eine Aufruferrolle im primären Konto

1. Öffnen Sie die IAM-Konsole unter `https://console.aws.amazon.com/iam/`.
2. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen aus.
3. Wählen Sie Benutzerdefinierte Vertrauensrichtlinie aus, kopieren Sie die folgende Richtlinie in das Fenster Benutzerdefinierte Vertrauensrichtlinie und klicken Sie dann auf Weiter.

> **Note**
>
> Wenn sich Ihre Ressourcen in unterschiedlichen Konten befinden, müssen Sie für jedes dieser Konten eine Rolle erstellen und die Vertrauensrichtlinie für sekundäre Konten für die anderen Konten verwenden.

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

4. Geben Sie auf der Seite „Berechtigungen hinzufügen“ **`AWSResilienceHubAsssessmentExecutionPolicy`** im Abschnitt „Berechtigungsrichtlinien“

das Feld Richtlinien nach Eigenschaft oder Richtliniennamen filtern ein und drücken Sie die Eingabetaste.

5. Wählen Sie die Richtlinie aus und klicken Sie auf Weiter.
6. Geben Sie im Abschnitt Rollendetails einen eindeutigen Rollennamen (z. B.`AWSResilienceHubAssessmentRole`) in das Feld Rollenname ein.

   Dieses Feld akzeptiert nur alphanumerische Zeichen und '`+=,.@-_/`' Zeichen.
7. (Optional) Geben Sie im Feld Beschreibung eine Beschreibung der Rolle ein.
8. Wählen Sie Create Role aus.

   Um die Anwendungsfälle und Berechtigungen zu bearbeiten, klicken Sie in Schritt 6 auf die Schaltfläche Bearbeiten, die sich rechts neben Schritt 1: Vertrauenswürdige Entitäten auswählen oder Schritt 2: Berechtigungsbereiche hinzufügen befindet.

Nachdem Sie die Aufruferrolle und die Ressourcenrolle (falls zutreffend) erstellt haben, können Sie Ihre Anwendung so konfigurieren, dass sie diese Rollen verwendet.

> **Note**
>
> Sie müssen in Ihrem aktuellen IAM Benutzer/Ihrer aktuellen Rolle über eine `iam:passRole` Berechtigung für die Aufruferrolle verfügen, wenn Sie die Anwendung erstellen oder aktualisieren. Sie benötigen diese Berechtigung jedoch nicht, um eine Bewertung durchzuführen.

Rollen verwalten mit dem IAM API

Die Vertrauensrichtlinie einer Rolle erteilt dem angegebenen Prinzipal die Erlaubnis, die Rolle zu übernehmen. Verwenden Sie den `create-role` Befehl, um die Rollen mit AWS Command Line Interface (AWS CLI) zu erstellen. Bei Verwendung dieses Befehls können Sie die Vertrauensrichtlinie direkt angeben. Das folgende Beispiel zeigt, wie Sie dem AWS Resilience Hub Dienst die Hauptberechtigung erteilen, Ihre Rolle zu übernehmen.

> **Note**
>
> Die Anforderung, Anführungszeichen (`' '`) in der JSON Zeichenfolge zu umgehen, kann je nach Ihrer Shell-Version variieren.

Beispiel **`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"
    }
  ]
}'
```

Definition einer Vertrauensrichtlinie mithilfe einer JSON Datei

Sie können die Vertrauensrichtlinie für die Rolle mithilfe einer separaten JSON Datei definieren und dann den `create-role` Befehl ausführen. Im folgenden Beispiel **`trust-policy.json`**befindet sich eine Datei, die die Vertrauensrichtlinie im aktuellen Verzeichnis enthält. Diese Richtlinie wird durch Ausführen eines **`create-role`**Befehls an eine Rolle angehängt. Die Ausgabe des **`create-role`** Befehls wird in der Beispielausgabe angezeigt. Verwenden Sie den attach-policy-to-roleBefehl, um der Rolle Berechtigungen hinzuzufügen, und Sie können damit beginnen, die `AWSResilienceHubAsssessmentExecutionPolicy` verwaltete Richtlinie hinzuzufügen. Weitere Informationen zu dieser verwalteten Richtlinie finden Sie unterthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Beispiel **`trust-policy.json`**

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

Stichprobe **`create-role`**

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

Beispielausgabe

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole",
        "CreateDate": "2020-01-17T23:19:12Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [{
                "Effect": "Allow",
                "Principal": {
                    "Service": "resiliencehub.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }]
        }
    }
}
```

Beispiel **`attach-policy-to-role`**

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

Rollen in verschiedenen AWS Konten für kontoübergreifenden Zugriff — optional

Wenn sich Ihre Ressourcen in sekundären Konten oder Ressourcenkonten befinden, müssen Sie in jedem dieser Konten Rollen erstellen, damit Ihre Anwendung erfolgreich bewertet werden AWS Resilience Hub kann. Das Verfahren zur Rollenerstellung ähnelt dem Verfahren zur Erstellung der Aufruferrolle, mit Ausnahme der Konfiguration der Vertrauensrichtlinie.

> **Note**
>
> Sie müssen die Rollen in sekundären Konten erstellen, in denen sich die Ressourcen befinden.

Topics

In der IAM Konsole eine Rolle für Sekundär-/Ressourcenkonten erstellen

Um den Zugriff auf AWS Dienste und Ressourcen in anderen AWS Konten AWS Resilience Hub zu ermöglichen, müssen Sie in jedem dieser Konten Rollen erstellen.

Um mithilfe der Konsole eine Rolle in der IAM Konsole für die sekundären Konten bzw. Ressourcenkonten zu erstellen IAM

1. Öffnen Sie die IAM-Konsole unter `https://console.aws.amazon.com/iam/`.
2. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen aus.
3. Wählen Sie Benutzerdefinierte Vertrauensrichtlinie aus, kopieren Sie die folgende Richtlinie in das Fenster Benutzerdefinierte Vertrauensrichtlinie und klicken Sie dann auf Weiter.

   > **Note**
   >
   > Wenn sich Ihre Ressourcen in verschiedenen Konten befinden, müssen Sie für jedes dieser Konten eine Rolle erstellen und die Vertrauensrichtlinie für sekundäre Konten für die anderen Konten verwenden.

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

```
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Geben Sie auf der Seite „Berechtigungen hinzufügen“ **`AWSResilienceHubAsssessmentExecutionPolicy`** im Abschnitt „Berechtigungsrichtlinien“ das Feld Richtlinien nach Eigenschaft oder Richtliniennamen filtern ein und drücken Sie die Eingabetaste.
5. Wählen Sie die Richtlinie aus und klicken Sie auf Weiter.
6. Geben Sie im Abschnitt Rollendetails einen eindeutigen Rollennamen (z. B.`AWSResilienceHubAssessmentRole`) in das Feld Rollenname ein.
7. (Optional) Geben Sie im Feld Beschreibung eine Beschreibung der Rolle ein.
8. Wählen Sie Create Role aus.

   Um die Anwendungsfälle und Berechtigungen zu bearbeiten, klicken Sie in Schritt 6 auf die Schaltfläche Bearbeiten, die sich rechts neben Schritt 1: Vertrauenswürdige Entitäten auswählen oder Schritt 2: Berechtigungsbereiche hinzufügen befindet.

Darüber hinaus müssen Sie der Aufruferrolle die `sts:assumeRole` Berechtigung hinzufügen, damit sie die Rollen in Ihren sekundären Konten übernehmen kann.

Fügen Sie Ihrer Aufruferrolle für jede der von Ihnen erstellten sekundären Rollen die folgende Richtlinie hinzu:

```
{
    "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"
      ]
```

```
}
```

Rollen verwalten mit dem IAM API

Die Vertrauensrichtlinie einer Rolle erteilt dem angegebenen Prinzipal die Erlaubnis, die Rolle zu übernehmen. Verwenden Sie den `create-role` Befehl, um die Rollen mit AWS Command Line Interface (AWS CLI) zu erstellen. Wenn Sie diesen Befehl verwenden, können Sie die Vertrauensrichtlinie angeben. Das folgende Beispiel zeigt, wie Sie dem AWS Resilience Hub Dienstprinzipal die Erlaubnis erteilen, Ihre Rolle anzunehmen.

> **Note**
>
> Die Anforderung, Anführungszeichen (`'  '`) in der JSON Zeichenfolge zu umgehen, kann je nach Ihrer Shell-Version variieren.

Beispiel **`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"}]}'
```

Sie können die Vertrauensrichtlinie für die Rolle auch mithilfe einer separaten JSON Datei definieren. Im folgenden Beispiel ist `trust-policy.json` eine Datei im aktuellen Verzeichnis.

Definition der Vertrauensrichtlinie mithilfe einer JSON Datei

Sie können die Vertrauensrichtlinie für die Rolle mithilfe einer separaten JSON Datei definieren und dann den `create-role` Befehl ausführen. Im folgenden Beispiel **`trust-policy.json`**befindet sich eine Datei, die die Vertrauensrichtlinie im aktuellen Verzeichnis enthält. Diese Richtlinie wird durch Ausführen eines **`create-role`**Befehls an eine Rolle angehängt. Die Ausgabe des **`create-role`** Befehls wird in der Beispielausgabe angezeigt. Verwenden Sie den attach-policy-to-roleBefehl, um einer Rolle Berechtigungen hinzuzufügen, und Sie können damit beginnen, die `AWSResilienceHubAsssessmentExecutionPolicy` verwaltete Richtlinie hinzuzufügen. Weitere Informationen zu dieser verwalteten Richtlinie finden Sie unterthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Beispiel **`trust-policy.json`**

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

Stichprobe **`create-role`**

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

Beispielausgabe

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole2",
        "RoleId": "AROAT2GICMEDJML6EVQRG",
        "Arn": "arn:aws:iam::262412591366:role/AWSResilienceHubAssessmentRole2",
        "CreateDate": "2023-08-02T07:49:23+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": [
                            "arn:aws:iam::262412591366:role/
AWSResilienceHubAssessmentRole"
                        ]
                    },
                    "Action": "sts:AssumeRole"
                }
```

```
            ]
        }
    }
}
```

Beispiel **`attach-policy-to-role`**

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

Aktuelle IAM Benutzerberechtigungen verwenden

Verwenden Sie diese Methode, wenn Sie Ihre aktuellen IAM Benutzerberechtigungen verwenden möchten, um eine Bewertung zu erstellen und auszuführen. Sie können die `AWSResilienceHubAsssessmentExecutionPolicy` verwaltete Richtlinie Ihrem IAM Benutzer oder einer Rolle zuordnen, die Ihrem Benutzer zugeordnet ist.

Einrichtung eines einzelnen Kontos

Die Verwendung der oben genannten verwalteten Richtlinie reicht aus, um eine Bewertung für eine Anwendung durchzuführen, die unter demselben Konto wie der IAM Benutzer verwaltet wird.

Einrichtung einer geplanten Bewertung

Sie müssen eine neue Rolle erstellen`AwsResilienceHubPeriodicAssessmentRole`, um geplante Aufgaben im Zusammenhang mit der Bewertung durchführen AWS Resilience Hub zu können.

> **Note**
>
> - Bei Verwendung des rollenbasierten Zugriffs (mit der oben genannten Aufruferrolle) ist dieser Schritt nicht erforderlich.
> - Der Rollenname muss sein. `AwsResilienceHubPeriodicAssessmentRole`

Um die Durchführung von geplanten Aufgaben im Zusammenhang mit der Bewertung AWS Resilience Hub zu ermöglichen

1. Hängen Sie die `AWSResilienceHubAsssessmentExecutionPolicy` verwaltete Richtlinie an die Rolle an.
2. Fügen Sie die folgende Richtlinie hinzu, in der `primary_account_id` sich das AWS Konto befindet, für das die Anwendung definiert ist und die Bewertung durchführt. Darüber hinaus müssen Sie die zugehörige Vertrauensrichtlinie (`AwsResilienceHubPeriodicAssessmentRole`) für die Rolle der geplanten Bewertung hinzufügen, die dem AWS Resilience Hub Dienst die Rechte gibt, die Rolle der geplanten Bewertung zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAdminAccountRole"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAssessmentEKSAccessRole"
      ]
    }
  ]
}
```

Vertrauensrichtlinie für die Rolle der geplanten Bewertung (**`AwsResilienceHubPeriodicAssessmentRole`**)

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

Kontoübergreifende Einrichtung

Die folgenden IAM Berechtigungsrichtlinien sind erforderlich, wenn Sie AWS Resilience Hub mit mehreren Konten verwenden. Für jedes AWS Konto sind je nach Anwendungsfall möglicherweise unterschiedliche Berechtigungen erforderlich. AWS Resilience Hub Bei der Einrichtung des kontoübergreifenden Zugriffs werden die folgenden Konten und Rollen berücksichtigt:

- Primärkonto — AWS Konto, in dem Sie die Anwendung erstellen und Bewertungen ausführen möchten.
- Sekundäres Konto/Ressourcenkonto (e) — AWS Konto (e), in dem sich die Ressourcen befinden.

> **Note**
>
> - Bei Verwendung des rollenbasierten Zugriffs (mit der oben genannten Aufruferrolle) ist dieser Schritt nicht erforderlich.
> - Weitere Informationen zur Konfiguration von Berechtigungen für den Zugriff auf Amazon Elastic Kubernetes Service finden Sie unter. the section called “ AWS Resilience Hub Zugriff auf Ihren EKS Amazon-Cluster aktivieren”

Einrichtung des primären Kontos

Sie müssen eine neue Rolle `AwsResilienceHubAdminAccountRole` im Hauptkonto erstellen und den AWS Resilience Hub Zugriff aktivieren, um diese Rolle übernehmen zu können. Diese Rolle wird

verwendet, um auf eine andere Rolle in Ihrem AWS Konto zuzugreifen, die Ihre Ressourcen enthält. Sie sollte keine Berechtigungen zum Lesen von Ressourcen haben.

> **Note**
>
> - Der Rollenname muss sein`AwsResilienceHubAdminAccountRole`.
> - Er muss im Hauptkonto erstellt werden.
> - Ihr aktueller IAM Benutzer/Ihre aktuelle Rolle muss über die `iam:assumeRole` Berechtigung verfügen, diese Rolle zu übernehmen.
> - Ersetzen Sie es `secondary_account_id_1/2/...` durch die entsprechenden sekundären Kontokennungen.

Die folgende Richtlinie gewährt Ihrer Rolle Ausführungsberechtigungen für den Zugriff auf Ressourcen in einer anderen Rolle in Ihrem Konto: AWS

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::secondary_account_id_1:role/AwsResilienceHubExecutorAccountRole",
        "arn:aws:iam::secondary_account_id_2:role/AwsResilienceHubExecutorAccountRole",
        ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

Die Vertrauensrichtlinie für die Administratorrolle (`AwsResilienceHubAdminAccountRole`) lautet wie folgt:

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

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

Einrichtung von Sekundär-/Ressourcenkonten

In jedem Ihrer sekundären Konten müssen Sie ein neues erstellen `AwsResilienceHubExecutorAccountRole` und die oben erstellte Administratorrolle aktivieren, um diese Rolle übernehmen zu können. Da diese Rolle von verwendet wird AWS Resilience Hub , um Ihre Anwendungsressourcen zu scannen und zu bewerten, sind auch die entsprechenden Berechtigungen erforderlich.

Sie müssen jedoch die `AWSResilienceHubAsssessmentExecutionPolicy` verwaltete Richtlinie an die Rolle anhängen und die Richtlinie für die Rolle des Ausführers anhängen.

Die Vertrauensrichtlinie für die Rolle des Ausführers lautet wie folgt:

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

```
}
```

AWS verwaltete Richtlinien für AWS Resilience Hub

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Denken Sie daran, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS -Service wird oder neue API Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

AWSResilienceHubAsssessmentExecutionPolicy

Sie können sie `AWSResilienceHubAsssessmentExecutionPolicy` an Ihre IAM Identitäten anhängen. Während der Durchführung einer Bewertung gewährt diese Richtlinie anderen AWS Diensten Zugriffsberechtigungen für die Durchführung von Bewertungen.

Berechtigungsdetails

Diese Richtlinie bietet angemessene Berechtigungen zum Veröffentlichen von Alarmen AWS FIS und SOP Vorlagen in Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket. Der Amazon S3 S3-Bucket-Name muss mit beginnen`aws-resilience-hub-artifacts-`. Wenn Sie in einem anderen Amazon S3 S3-Bucket veröffentlichen möchten, können Sie dies während des Anrufs tun `CreateRecommendationTemplate`API. Weitere Informationen finden Sie unter CreateRecommendationTemplate.

Diese Richtlinie umfasst die folgenden Berechtigungen:

- Amazon CloudWatch (CloudWatch) — Ruft alle implementierten Alarme ab, die Sie in Amazon eingerichtet haben CloudWatch , um die Anwendung zu überwachen. Darüber hinaus veröffentlichen wir CloudWatch Metriken für den Resilienz-Score der Anwendung im `ResilienceHub` Namespace. `cloudwatch:PutMetricData`
- Amazon Data Lifecycle Manager — Ruft `Describe` Berechtigungen für Amazon Data Lifecycle Manager Manager-Ressourcen ab, die Ihrem AWS Konto zugeordnet sind, und gewährt diese.
- Amazon DevOps Guru — Listet Amazon DevOps Guru-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und gewährt `Describe` Berechtigungen für diese.
- Amazon DocumentDB — Listet Amazon DocumentDB DocumentDB-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und bietet `Describe` Berechtigungen für diese.
- Amazon DynamoDB (DynamoDB) — Listet Amazon DynamoDB DynamoDB-Ressourcen auf, die mit Ihrem Konto verknüpft sind, und stellt `Describe` Berechtigungen bereit. AWS
- Amazon ElastiCache (ElastiCache) — Stellt `Describe` Berechtigungen für ElastiCache Ressourcen bereit, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic Compute Cloud (AmazonEC2) — Listet Amazon-Ressourcen auf und bietet `Describe` Berechtigungen für diese EC2 Ressourcen, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic Container Registry (AmazonECR) — Stellt `Describe` Berechtigungen für ECR Amazon-Ressourcen bereit, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic Container Service (AmazonECS) — Stellt `Describe` Berechtigungen für ECS Amazon-Ressourcen bereit, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic File System (AmazonEFS) — Stellt `Describe` Berechtigungen für EFS Amazon-Ressourcen bereit, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic Kubernetes Service (AmazonEKS) — Listet EKS Amazon-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und bietet `Describe` Berechtigungen für diese.
- Amazon EC2 Auto Scaling — Listet Amazon Auto Scaling-Ressourcen auf und bietet `Describe` Berechtigungen für Amazon EC2 Auto Scaling Scaling-Ressourcen, die mit Ihrem AWS Konto verknüpft sind.
- Amazon EC2 Systems Manager (SSM) — Stellt `Describe` Berechtigungen für SSM Ressourcen bereit, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Fault Injection Service (AWS FIS) — Listet AWS FIS Experimente und Versuchsvorlagen auf, die mit Ihrem AWS Konto verknüpft sind, und gewährt `Describe` Genehmigungen für diese.

- Amazon FSx für Windows File Server (AmazonFSx) — Listet FSx Amazon-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und bietet `Describe` Berechtigungen für diese.
- Amazon RDS — Listet RDS Amazon-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und gewährt `Describe` Berechtigungen für diese.
- Amazon Route 53 (Route 53) — Listet Route 53-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und bietet `Describe` Berechtigungen für diese.
- Amazon Route 53 Resolver — Listet Amazon Route 53 Resolver Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und stellt `Describe` Berechtigungen für diese bereit.
- Amazon Simple Notification Service (AmazonSNS) — Listet SNS Amazon-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und bietet `Describe` Berechtigungen für diese.
- Amazon Simple Queue Service (AmazonSQS) — Listet SQS Amazon-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und gewährt `Describe` Berechtigungen für diese.
- Amazon Simple Storage Service (Amazon S3) — Listet Amazon S3 S3-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und stellt `Describe` Berechtigungen bereit.

> **Note**
>
> Wenn während der Durchführung einer Bewertung Berechtigungen fehlen, die aus den verwalteten Richtlinien aktualisiert werden müssen, AWS Resilience Hub wird die Bewertung mithilfe der s3: GetBucketLogging -Berechtigung erfolgreich abgeschlossen. Es AWS Resilience Hub wird jedoch eine Warnmeldung angezeigt, in der die fehlenden Berechtigungen aufgeführt sind, und es wird eine Frist eingeräumt, um sie hinzuzufügen. Wenn Sie die fehlenden Berechtigungen nicht innerhalb der angegebenen Nachfrist hinzufügen, schlägt die Bewertung fehl.

- AWS Backup — Listet Amazon EC2 Auto Scaling Scaling-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und ruft `Describe` Berechtigungen für diese ab.
- AWS CloudFormation — Listet Ressourcen auf AWS CloudFormation Stacks auf, die mit Ihrem AWS Konto verknüpft sind, und ruft `Describe` Berechtigungen für diese ab.
- AWS DataSync — Listet AWS DataSync Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und stellt `Describe` Berechtigungen für diese bereit.
- AWS Directory Service — Listet AWS Directory Service Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und stellt `Describe` Berechtigungen für diese bereit.
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery) — Stellt `Describe` Berechtigungen für Elastic Disaster Recovery-Ressourcen bereit, die Ihrem AWS Konto zugeordnet sind.

- AWS Lambda (Lambda) — Listet Lambda-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und bietet `Describe` Berechtigungen für diese.
- AWS Resource Groups (Resource Groups) — Listet Ressourcengruppen-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und bietet `Describe` Berechtigungen für diese Ressourcen.
- AWS Service Catalog (Service Catalog) — Listet Service Catalog-Ressourcen auf, die Ihrem AWS Konto zugeordnet sind, und bietet `Describe` Berechtigungen für diese.
- AWS Step Functions — Listet AWS Step Functions Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und stellt `Describe` Berechtigungen für diese bereit.
- Elastic Load Balancing — Listet Elastic Load Balancing Balancing-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und stellt `Describe` Berechtigungen bereit.
- `ssm:GetParametersByPath`— Wir verwenden diese Berechtigung, um CloudWatch Alarme, Tests oder solche, SOPs die für Ihre Anwendung konfiguriert sind, zu verwalten.

Die folgende IAM Richtlinie ist für ein AWS Konto erforderlich, um Berechtigungen für Benutzer, Benutzergruppen und Rollen hinzuzufügen, die Ihrem Team die erforderlichen Berechtigungen für den Zugriff auf AWS Dienste während der Durchführung von Assessments gewähren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSResilienceHubFullResourceStatement",
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:DescribeScalableTargets",
                "autoscaling:DescribeAutoScalingGroups",
                "backup:DescribeBackupVault",
                "backup:GetBackupPlan",
                "backup:GetBackupSelection",
                "backup:ListBackupPlans",
                "backup:ListBackupSelections",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "datasync:DescribeTask",
                "datasync:ListLocations",
```

```
                "datasync:ListTasks",
                "devops-guru:ListMonitoredResources",
                "dlm:GetLifecyclePolicies",
                "dlm:GetLifecyclePolicy",
                "docdb-elastic:GetCluster",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:ListTagsForResource",
                "drs:DescribeJobs",
                "drs:DescribeSourceServers",
                "drs:GetReplicationConfiguration",
                "ds:DescribeDirectories",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:DescribeGlobalTable",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTagsOfResource",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeFleets",
                "ec2:DescribeHosts",
                "ec2:DescribeInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcEndpoints",
                "ecr:DescribeRegistry",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeClusters",
                "ecs:DescribeContainerInstances",
                "ecs:DescribeServices",
                "ecs:DescribeTaskDefinition",
                "ecs:ListContainerInstances",
                "ecs:ListServices",
                "eks:DescribeCluster",
                "eks:DescribeFargateProfile",
                "eks:DescribeNodegroup",
                "eks:ListFargateProfiles",
                "eks:ListNodegroups",
```

```
                "elasticache:DescribeCacheClusters",
                "elasticache:DescribeGlobalReplicationGroups",
                "elasticache:DescribeReplicationGroups",
                "elasticache:DescribeSnapshots",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "fis:GetExperimentTemplate",
                "fis:ListExperimentTemplates",
                "fis:ListExperiments",
                "fsx:DescribeFileSystems",
                "lambda:GetFunctionConcurrency",
                "lambda:GetFunctionConfiguration",
                "lambda:ListAliases",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctionEventInvokeConfigs",
                "lambda:ListVersionsByFunction",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeDBProxies",
                "rds:DescribeDBProxyTargets",
                "rds:DescribeDBSnapshots",
                "rds:DescribeGlobalClusters",
                "rds:ListTagsForResource",
                "resource-groups:GetGroup",
                "resource-groups:ListGroupResources",
                "route53-recovery-control-config:ListClusters",
                "route53-recovery-control-config:ListControlPanels",
                "route53-recovery-control-config:ListRoutingControls",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
```

```
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:ListBucket",
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources",
                "sns:GetSubscriptionAttributes",
                "sns:GetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sqs:GetQueueAttributes",
                "sqs:GetQueueUrl",
                "ssm:DescribeAutomationExecutions",
                "states:DescribeStateMachine",
                "states:ListStateMachineVersions",
                "states:ListStateMachineAliases",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSResilienceHubApiGatewayStatement",
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/apis/*",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/usageplans"
            ]
        },
        {
            "Sid": "AWSResilienceHubS3ArtifactStatement",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
```

```
        {
            "Sid": "AWSResilienceHubS3AccessStatement",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetMultiRegionAccessPointRoutes",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubCloudWatchStatement",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "ResilienceHub"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubSSMStatement",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
        }
    ]
```

```
}
```

AWS Resilience Hub Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS Resilience Hub seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS Feed auf der Seite AWS Resilience Hub Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWSResilienceHubAssessmentExecutionPolicy— Ändern	AWS Resilience Hub aktualisiert `AWSResilienceHubAssessmentExecutionPolicy` , um Ihnen `Describe` Berechtigungen zu gewähren, mit denen Sie auf Ressourcen und Konfigurationen in Amazon DocumentDB, Elastic Load Balancing und AWS Lambda während der Durchführung von Bewertungen zugreifen können.	01. August 2024
AWSResilienceHubAssessmentExecutionPolicy— Veränderung	AWS Resilience Hub aktualisiert `AWSResilienceHubAsssessmentExecutionPolicy` , um Ihnen `Describe` Berechtigungen zu gewähren, die es Ihnen ermöglichen, die Dateiserverkonfiguration von Amazon FSx für Windows während der Durchführung von Bewertungen zu lesen.	26. März 2024

Änderung	Beschreibung	Datum
AWSResilienceHubAssessmentExecutionPolicy— Veränderung	AWS Resilience Hub wurde aktualisiert `AWSResilienceHubAsssessmentExecutionPolicy` und gewährt `Describe` nun Berechtigungen, mit denen Sie die AWS Step Functions Konfiguration während der Durchführung von Bewertungen lesen können.	30. Oktober 2023
AWSResilienceHubAssessmentExecutionPolicy— Ändern	AWS Resilience Hub aktualisiert`AWSResilienceHubAsssessmentExecutionPolicy` , um Ihnen `Describe` Berechtigungen zu gewähren, damit Sie RDS während der Durchführung von Bewertungen auf Ressourcen bei Amazon zugreifen können.	05. Oktober 2023
AWSResilienceHubAssessmentExecutionPolicy— Neu	Diese AWS Resilience Hub Richtlinie bietet Zugriff auf andere AWS Dienste für die Durchführung von Bewertungen.	26. Juni 2023
AWS Resilience Hub hat begonnen, Änderungen zu verfolgen	AWS Resilience Hub hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	15. Juni 2023

AWS Resilience Hub Referenz zu Personas und IAM Berechtigungen

Mithilfe `AWSResilienceHubAsssessmentExecutionPolicy` AWS verwalteter Richtlinien und einer der folgenden personenspezifischen Richtlinien können Sie Personas die für die Arbeit erforderlichen IAM Berechtigungen gewähren. AWS Resilience Hub Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter. the section called “AWSResilienceHubAsssessmentExecutionPolicy”

Richtlinien für Personas, vorgeschlagen von AWS Resilience Hub:

- IAMBerechtigungen für Infrastructure Application Manager Persona
- IAMBerechtigungen für die Business Continuity Manager-Persona
- IAMBerechtigungen für die Persona des Anwendungsbesitzers
- IAMBerechtigungen für die Gewährung von schreibgeschütztem Zugriff

IAMBerechtigungen für Infrastructure Application Manager Persona

Die folgende Richtlinie gewährt die erforderlichen Berechtigungen, die für die Infrastructure Application Manager-Persona erforderlich sind.

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

IAMBerechtigungen für die Business Continuity Manager-Persona

Die folgende Richtlinie gewährt die erforderlichen Berechtigungen für die Business Continuity Manager-Persona.

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

IAMBerechtigungen für die Persona des Anwendungsbesitzers

Die folgende Richtlinie gewährt die erforderlichen Berechtigungen, die für die Persona des Anwendungsbesitzers erforderlich sind.

```
{
  "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": "*"
```

```
    }
  ]
}
```

IAMBerechtigungen für die Gewährung von schreibgeschütztem Zugriff

Die folgende Richtlinie gewährt die erforderlichen Berechtigungen, die für den schreibgeschützten Zugriff erforderlich sind.

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

Terraform-Statusdatei importieren in AWS Resilience Hub

AWS Resilience Hub unterstützt den Import von Terraform-Statusdateien, die mit serverseitiger Verschlüsselung (SSE) mit von Amazon Simple Storage Service verwalteten Schlüsseln (SSE-S3) oder mit AWS Key Management Service verwalteten Schlüsseln (-) verschlüsselt wurden. SSE KMS Wenn Ihre Terraform-Statusdateien mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C) verschlüsselt sind, können Sie sie nicht mit importieren. AWS Resilience Hub

Für den Import von Terraform-Statusdateien in AWS Resilience Hub sind die folgenden IAM Richtlinien erforderlich, je nachdem, wo sich Ihre Statusdatei befindet.

Terraform-Statusdateien aus einem Amazon S3 S3-Bucket importieren, der sich im Hauptkonto befindet

Die folgenden Amazon S3 S3-Bucket-Richtlinien und IAM -Richtlinien sind erforderlich, um den AWS Resilience Hub Lesezugriff auf Ihre Terraform-Statusdateien zu ermöglichen, die sich in einem Amazon S3 S3-Bucket auf dem primären Konto befinden.

- Bucket-Richtlinie — Eine Bucket-Richtlinie für den Amazon S3 S3-Ziel-Bucket, der sich im primären Konto befindet. Weitere Informationen finden Sie im folgenden Beispiel.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

- Identitätsrichtlinie — Die zugehörige Identitätsrichtlinie für die Invoker-Rolle, die für diese Anwendung definiert wurde, oder die AWS aktuelle IAM Rolle AWS Resilience Hub auf dem primären AWS Konto. Weitere Informationen finden Sie im folgenden Beispiel.

```
{
  "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**
>
> Wenn Sie die `AWSResilienceHubAsssessmentExecutionPolicy` verwaltete Richtlinie verwenden, ist keine `ListBucket` Genehmigung erforderlich.

> **Note**
>
> Wenn Ihre Terraform-Statusdateien mit verschlüsselt sindKMS, müssen Sie die folgende `kms:Decrypt` Berechtigung hinzufügen.

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

Terraform-Statusdateien aus einem Amazon S3 S3-Bucket importieren, der sich in einem sekundären Konto befindet

- Bucket-Richtlinie — Eine Bucket-Richtlinie für den Amazon S3 S3-Ziel-Bucket, der sich in einem der sekundären Konten befindet. Weitere Informationen finden Sie im folgenden Beispiel.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

- Identitätsrichtlinie — Die zugehörige Identitätsrichtlinie für die AWS Kontorolle, die AWS Resilience Hub auf dem primären AWS Konto ausgeführt wird. Weitere Informationen finden Sie im folgenden Beispiel.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

> **Note**
>
> Wenn Sie die `AWSResilienceHubAsssessmentExecutionPolicy` verwaltete Richtlinie verwenden, ist keine `ListBucket` Genehmigung erforderlich.

> **Note**
>
> Wenn Ihre Terraform-Statusdateien mit verschlüsselt sindKMS, müssen Sie die folgende `kms:Decrypt` Berechtigung hinzufügen.

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

AWS Resilience Hub Zugriff auf Ihren Amazon Elastic Kubernetes Service Service-Cluster aktivieren

AWS Resilience Hub bewertet die Resilienz eines Amazon Elastic Kubernetes Service (AmazonEKS) -Clusters, indem die Infrastruktur Ihres Amazon-Clusters analysiert wird. EKS AWS Resilience Hub verwendet die rollenbasierte Zugriffskontrollkonfiguration (RBAC) von Kubernetes, um andere Kubernetes (K8s) -Workloads zu bewerten, die als Teil des Amazon-Clusters bereitgestellt werden.

EKS AWS Resilience Hub Um Ihren EKS Amazon-Cluster zur Analyse und Bewertung der Arbeitslast abzufragen, müssen Sie die folgenden Schritte ausführen:

- Erstellen oder verwenden Sie eine bestehende Rolle AWS Identity and Access Management (IAM) in demselben Konto wie der EKS Amazon-Cluster.
- Ermöglichen Sie IAM Benutzer- und Rollenzugriff auf Ihren EKS Amazon-Cluster und gewähren Sie zusätzliche Nur-Lese-Berechtigungen für K8s-Ressourcen innerhalb des Amazon-Clusters. EKS Weitere Informationen zur Aktivierung des IAM Benutzer- und Rollenzugriffs auf Ihren EKS Amazon-Cluster finden Sie unter Aktivieren des IAM Benutzer- und Rollenzugriffs auf Ihren Cluster — Amazon EKS.

Der Zugriff auf Ihren EKS Amazon-Cluster mithilfe von IAM Entitäten wird durch den AWS IAMAuthenticator for Kubernetes ermöglicht, der auf der EKS Amazon-Steuerebene ausgeführt wird. Der Authenticator bezieht die Konfigurationsinformationen von. `aws-auth ConfigMap`

> **Note**
>
> - Weitere Informationen zu allen `aws-auth ConfigMap` Einstellungen finden Sie unter Vollständiges Konfigurationsformat unter. GitHub
> - Weitere Informationen zu verschiedenen IAM Identitäten finden Sie unter Identitäten (Benutzer, Gruppen und Rollen) im IAM Benutzerhandbuch.
> - Weitere Informationen zur Konfiguration der rollenbasierten Zugriffskontrolle (RBAC) von Kubernetes finden Sie unter Autorisierung verwenden. RBAC

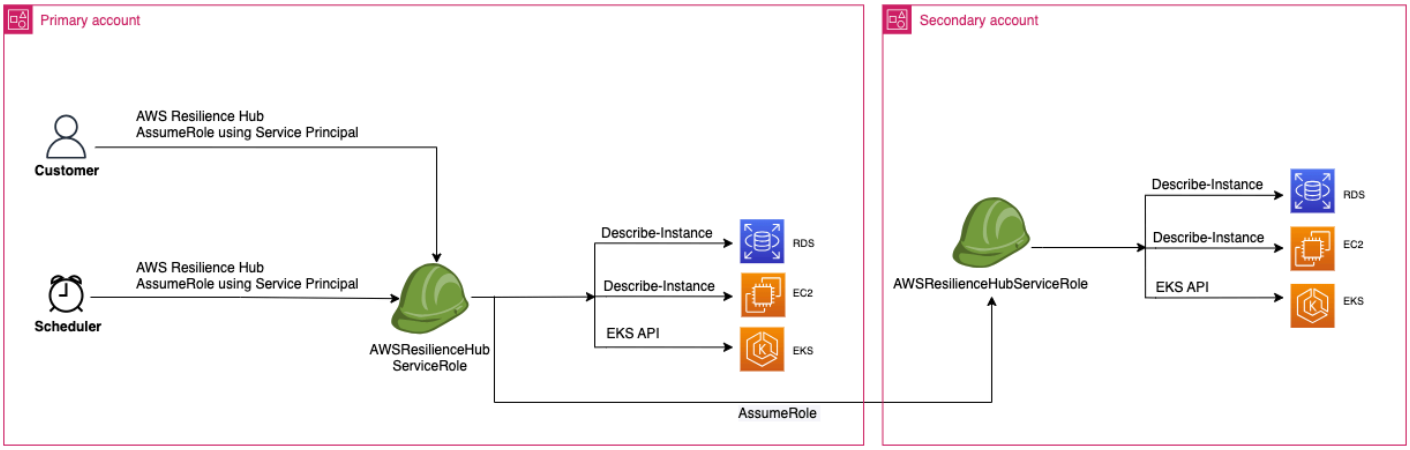
AWS Resilience Hub fragt Ressourcen in Ihrem EKS Amazon-Cluster mithilfe einer IAM Rolle in Ihrem Konto ab. Damit Sie AWS Resilience Hub auf Ressourcen in Ihrem EKS Amazon-Cluster zugreifen können, AWS Resilience Hub muss die von verwendete IAM Rolle einer Kubernetes-Gruppe mit ausreichenden Leseberechtigungen für Ressourcen in Ihrem Amazon-Cluster zugeordnet sein. EKS

AWS Resilience Hub ermöglicht den Zugriff auf Ihre EKS Amazon-Cluster-Ressourcen mithilfe einer der folgenden IAM Rollenoptionen:

- Wenn Ihre Anwendung so konfiguriert ist, dass sie den rollenbasierten Zugriff für den Zugriff auf Ressourcen verwendet, wird die Aufruferrolle oder die sekundäre Kontorolle, an die Sie bei der

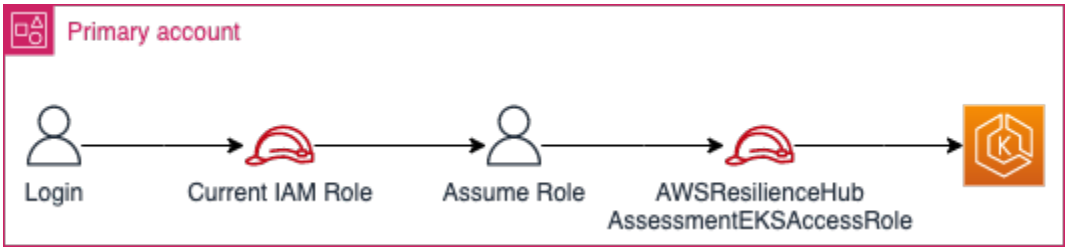
Erstellung einer Anwendung übergeben haben, AWS Resilience Hub während der Bewertung für den Zugriff auf Ihren EKS Amazon-Cluster verwendet.

Das folgende Konzeptdiagramm zeigt, wie AWS Resilience Hub auf EKS Amazon-Cluster zugegriffen wird, wenn die Anwendung als rollenbasierte Anwendung konfiguriert ist.

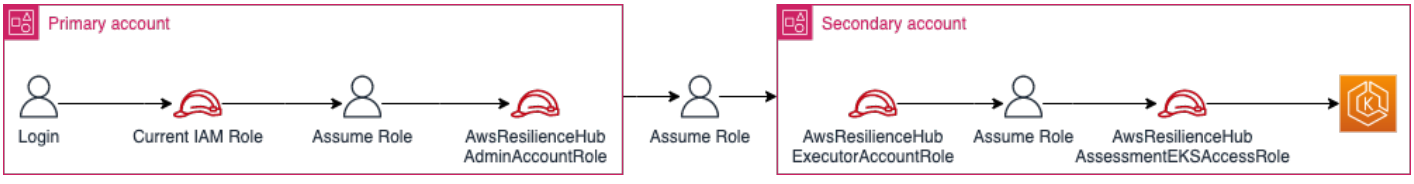


- Wenn Ihre Anwendung so konfiguriert ist, dass sie den aktuellen IAM Benutzer für den Zugriff auf Ressourcen verwendet, müssen Sie eine neue IAM Rolle mit dem Namen `AwsResilienceHubAssessmentEKSAccessRole` in demselben Konto wie dem des EKS Amazon-Clusters erstellen. Diese IAM Rolle wird dann für den Zugriff auf Ihren EKS Amazon-Cluster verwendet.

  Das folgende Konzeptdiagramm zeigt, wie auf EKS Amazon-Cluster AWS Resilience Hub zugegriffen wird, die in Ihrem primären Konto bereitgestellt werden, wenn die Anwendung so konfiguriert ist, dass sie die aktuellen IAM Benutzerberechtigungen verwendet.



  Das folgende Konzeptdiagramm zeigt, wie auf EKS Amazon-Cluster AWS Resilience Hub zugegriffen wird, die auf einem sekundären Konto bereitgestellt werden, wenn die Anwendung so konfiguriert ist, dass sie die aktuellen IAM Benutzerberechtigungen verwendet.



AWS Resilience Hub Zugriff auf Ressourcen in Ihrem EKS Amazon-Cluster gewähren

AWS Resilience Hub ermöglicht Ihnen den Zugriff auf Ressourcen, die sich auf EKS Amazon-Clustern befinden, sofern Sie die erforderlichen Berechtigungen konfiguriert haben.

Um die erforderlichen Berechtigungen AWS Resilience Hub für die Erkennung und Bewertung von Ressourcen innerhalb des EKS Amazon-Clusters zu erteilen

1. Konfigurieren Sie eine IAM Rolle für den Zugriff auf den EKS Amazon-Cluster.

   Wenn Sie Ihre Anwendung mit rollenbasiertem Zugriff konfiguriert haben, können Sie diesen Schritt überspringen und mit Schritt 2 fortfahren und die Rolle verwenden, die Sie für die Erstellung der Anwendung verwendet haben. Weitere Informationen zur AWS Resilience Hub Verwendung von IAM Rollen finden Sie unter. the section called “Wie funktioniert AWS Resilience Hub mit IAM”

   Wenn Sie Ihre Anwendung mit aktuellen IAM Benutzerberechtigungen konfiguriert haben, müssen Sie die `AwsResilienceHubAssessmentEKSAccessRole` IAM Rolle in demselben Konto wie das des EKS Amazon-Clusters erstellen. Diese IAM Rolle wird dann beim Zugriff auf Ihren EKS Amazon-Cluster verwendet.

   AWS Resilience Hub Verwendet beim Import und der Bewertung Ihrer Anwendung eine IAM Rolle, um auf die Ressourcen in Ihrem EKS Amazon-Cluster zuzugreifen. Diese Rolle sollte in demselben Konto wie Ihr EKS Amazon-Cluster erstellt werden. Sie wird einer Kubernetes-Gruppe zugeordnet, die die für die Bewertung Ihres Amazon-Clusters erforderlichen Berechtigungen enthält. AWS Resilience Hub EKS

   Wenn sich Ihr EKS Amazon-Cluster in demselben Konto wie das AWS Resilience Hub aufrufende Konto befindet, sollte die Rolle mithilfe der folgenden IAM Vertrauensrichtlinie erstellt werden. In dieser IAM Vertrauensrichtlinie `caller_IAM_role` wird im Girokonto verwendet, um den APIs für aufzurufen AWS Resilience Hub.

   > **Note**
   >
   > Das `caller_IAM_role` ist die Rolle, die Ihrem AWS Benutzerkonto zugeordnet ist.

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

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

Wenn sich Ihr EKS Amazon-Cluster in einem Cross-Konto befindet (ein anderes Konto als das AWS Resilience Hub aufrufende Konto), müssen Sie die `AwsResilienceHubAssessmentEKSAccessRole` IAM Rolle mithilfe der folgenden IAM Vertrauensrichtlinie erstellen:

> **Note**
>
> Als Voraussetzung für den Zugriff auf EKS Amazon-Cluster, der in einem anderen Konto als dem Konto des AWS Resilience Hub Benutzers bereitgestellt wird, müssen Sie den Zugriff mit mehreren Konten konfigurieren. Weitere Informationen finden Sie unter

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

2. Erstellen Sie Rollen `ClusterRole` und `ClusterRoleBinding` (oder`RoleBinding`) für die AWS Resilience Hub Anwendung.

Erstellt `ClusterRole` Ressourcen, die Teil bestimmter Namespaces in Ihrem AWS Resilience Hub Amazon-Cluster sind, und gewährt ihnen die erforderlichen Leseberechtigungen für die Analyse und Bewertung. `ClusterRoleBinding` EKS

AWS Resilience Hub ermöglicht es Ihnen, den Zugriff auf Ihre Namespaces für die Erstellung von Resilienzanalysen zu beschränken, indem Sie einen der folgenden Schritte ausführen:

a. Gewähren Sie der Anwendung Lesezugriff für alle Namespaces. AWS Resilience Hub

   AWS Resilience Hub Um die Resilienz von Ressourcen in allen Namespaces innerhalb eines EKS Amazon-Clusters zu bewerten, müssen Sie das folgende und erstellen. `ClusterRole` `ClusterRoleBinding`

   - `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — Definiert die Berechtigungen, die für die Bewertung Ihres EKS Amazon-Clusters erforderlich sind. AWS Resilience Hub
   - `resilience-hub-eks-access-cluster-role-binding`(`ClusterRoleBinding`) — Definiert eine `resilience-hub-eks-access-group` in Ihrem EKS Amazon-Cluster benannte Gruppe, die ihren Benutzern die erforderlichen Berechtigungen zur Durchführung von Resilienzanalysen gewährt. AWS Resilience Hub

   Die Vorlage, um der AWS Resilience Hub Anwendung Lesezugriff auf alle Namespaces zu gewähren, lautet wie folgt:

```
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. Gewährung AWS Resilience Hub des Zugriffs auf das Lesen bestimmter Namespaces.

Sie können AWS Resilience Hub den Zugriff auf Ressourcen innerhalb eines bestimmten Satzes von Namespaces einschränken, indem Sie. `RoleBinding` Um dies zu erreichen, müssen Sie die folgenden Rollen erstellen:

- `ClusterRole`— AWS Resilience Hub Um auf die Ressourcen in bestimmten Namespaces innerhalb eines EKS Amazon-Clusters zuzugreifen und dessen Resilienz zu bewerten, müssen Sie die folgenden Rollen erstellen. `ClusterRole`
  - `resilience-hub-eks-access-cluster-role`— Gibt die erforderlichen Berechtigungen an, um die Ressourcen in bestimmten Namespaces zu bewerten.
  - `resilience-hub-eks-access-global-cluster-role`— Gibt die erforderlichen Berechtigungen an, um clusterbezogene Ressourcen, die keinem bestimmten Namespace zugeordnet sind, innerhalb Ihrer Amazon-Cluster zu bewerten. EKS AWS Resilience Hub erfordert Berechtigungen für den Zugriff auf Ressourcen im Clusterbereich (z. B. Knoten) in Ihrem EKS Amazon-Cluster, um die Widerstandsfähigkeit Ihrer Anwendung beurteilen zu können.

  Die Vorlage zum Erstellen `ClusterRole` einer Rolle lautet wie folgt:

```
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`Rolle — Diese Rolle gewährt die erforderlichen Berechtigungen für den AWS Resilience Hub Zugriff auf Ressourcen in bestimmten Namespaces. Das heißt, Sie müssen in jedem Namespace `RoleBinding` eine Rolle erstellen, um auf Ressourcen innerhalb des angegebenen AWS Resilience Hub Namespaces zugreifen zu können.

  > **Note**
  >
  > Wenn Sie Autoscaling verwenden`ClusterAutoscaler`, müssen Sie zusätzlich in der erstellen`RoleBinding`. `kube-system` Dies ist notwendig, um Ihren`ClusterAutoscaler`, der Teil des `kube-system` Namespace ist, zu beurteilen.

Auf diese Weise gewähren Sie AWS Resilience Hub die erforderlichen Berechtigungen, um Ressourcen innerhalb des `kube-system` Namespace zu bewerten und gleichzeitig Ihren EKS Amazon-Cluster zu bewerten.

Die Vorlage zum Erstellen einer `RoleBinding` Rolle lautet wie folgt:

```
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`Rolle — Diese Rolle gewährt die erforderlichen Berechtigungen für den Zugriff AWS Resilience Hub auf Ressourcen im Clusterbereich.

  Die Vorlage zum Erstellen einer `ClusterRoleBinding` Rolle lautet wie folgt:

```
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. Aktualisieren Sie das`aws-auth ConfigMap`, um das der IAM Rolle `resilience-hub-eks-access-group` zuzuordnen, die für den Zugriff auf den EKS Amazon-Cluster verwendet wird.

   In diesem Schritt wird eine Zuordnung zwischen der in Schritt 1 verwendeten IAM Rolle und der in Schritt 2 erstellten Kubernetes-Gruppe erstellt. Diese Zuordnung gewährt IAM Rollen Berechtigungen für den Zugriff auf Ressourcen innerhalb des EKS Amazon-Clusters.

   > **Note**
   >
   > - `ROLE-NAME`bezieht sich auf die IAM Rolle, die für den Zugriff auf EKS Amazon-Cluster verwendet wird.
   >   - Wenn Ihre Anwendung für den rollenbasierten Zugriff konfiguriert ist, sollte es sich bei der Rolle entweder um die Rolle des Aufrufers oder um die Rolle des sekundären Kontos handeln, an die Sie bei der Erstellung der Anwendung übergeben AWS Resilience Hub werden.
   >   - Wenn Ihre Anwendung so konfiguriert ist, dass sie den aktuellen IAM Benutzer für den Zugriff auf Ressourcen verwendet, muss es sich um den. `AwsResilienceHubAssessmentEKSAccessRole`
   > - `ACCOUNT-ID`sollte die AWS Konto-ID des EKS Amazon-Clusters sein.

   Sie können das auf `aws-auth ConfigMap` eine der folgenden Arten erstellen:

   - Verwenden von `eksctl`

     Verwenden Sie den folgenden Befehl, um das zu aktualisieren `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
```

- Sie können manuell bearbeiten, `aws-auth` `ConfigMap` indem Sie die IAM Rollendetails zum `mapRoles` Abschnitt `ConfigMap` unter den Daten hinzufügen. Verwenden Sie den folgenden Befehl, um das zu bearbeiten `aws-auth``ConfigMap`.

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

  `mapRoles`Abschnitt besteht aus den folgenden Parametern:

  - `rolearn`— Der Amazon-Ressourcenname (ARN) der IAM Rolle, die hinzugefügt werden soll.
    - ARNSyntax —`arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
  - `username`— Der Benutzername in Kubernetes, der der IAM Rolle () zugeordnet werden soll. `AwsResilienceHubAssessmentEKSAccessRole`
  - `groups`— Die Gruppennamen sollten mit den in Schritt 2 () erstellten Gruppennamen übereinstimmen. `resilience-hub-eks-access-group`

  > **Note**
  >
  > Wenn der `mapRoles` Abschnitt nicht existiert, müssen Sie diesen Abschnitt manuell hinzufügen.

  Verwenden Sie die folgende Vorlage, um die IAM Rollendetails zum `mapRoles` Abschnitt der `ConfigMap` Unterdaten hinzuzufügen.

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

Aktivierung AWS Resilience Hub der Veröffentlichung in Ihren Amazon Simple Notification Service-Themen

In diesem Abschnitt wird erklärt, wie Sie die Veröffentlichung von Benachrichtigungen über die Anwendung in Ihren Amazon Simple Notification Service (AmazonSNS) -Themen aktivieren AWS Resilience Hub können. Um Push-Benachrichtigungen zu einem SNS Amazon-Thema zu senden, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Eine aktive AWS Resilience Hub Anwendung.
- Ein vorhandenes SNS Amazon-Thema, an das Benachrichtigungen gesendet AWS Resilience Hub werden müssen. Weitere Informationen zum Erstellen eines SNS Amazon-Themas finden Sie unter Ein SNS Amazon-Thema erstellen.

Um Benachrichtigungen AWS Resilience Hub zu Ihrem SNS Amazon-Thema veröffentlichen zu können, müssen Sie die Zugriffsrichtlinie für das SNS Amazon-Thema wie folgt aktualisieren:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubPublish",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name"
    }
  ]
}
```

> **Note**
>
> Wenn Sie AWS Resilience Hub bisher Nachrichten aus Regionen mit Opt-in-Status zu Themen veröffentlichen, die sich in Regionen befinden, die standardmäßig aktiviert sind, müssen Sie die für das SNS Amazon-Thema erstellte Ressourcenrichtlinie ändern. Ändern Sie den Wert von Principal von `resiliencehub.amazonaws.com` auf`resiliencehub.<opt-in-region>.amazonaws.com`.

Wenn Sie ein SNS Amazon-Thema mit serverseitiger Verschlüsselung (SSE) verwenden, müssen Sie sicherstellen, dass das Thema `Decrypt` und `GenerateDataKey` * Zugriff auf den SNS Amazon-Verschlüsselungsschlüssel AWS Resilience Hub hat.

Für die Bereitstellung `Decrypt` und `GenerateDataKey*` den Zugriff AWS Resilience Hub darauf müssen Sie die folgenden Richtlinien für Zugriffsberechtigungen angeben. AWS Key Management Service

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubDecrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id"
    }
  ]
}
```

Beschränken Sie die Berechtigungen auf das Ein- oder Ausschließen von AWS Resilience Hub Empfehlungen

AWS Resilience Hub ermöglicht es Ihnen, die Berechtigungen zum Ein- oder Ausschließen von Empfehlungen pro Anwendung einzuschränken. Mithilfe der folgenden IAM Vertrauensrichtlinie können Sie die Berechtigungen so einschränken, dass Empfehlungen pro Anwendung aufgenommen oder ausgeschlossen werden. In dieser IAM Vertrauensrichtlinie wird `caller_IAM_role` (mit Ihrem AWS Benutzerkonto verknüpft) im aktuellen Konto verwendet, um die APIs für aufzurufen AWS Resilience Hub.

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

```
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "resiliencehub:BatchUpdateRecommendationStatus",
      "Resource": "arn:aws:resiliencehub:us-west-2:12345678900:app/0e6237b7-23ba-4103-
adb2-91811326b703"
    }
  ]
}
```

Sicherheit der Infrastruktur in AWS Resilience Hub

Als verwalteter Service AWS Resilience Hub ist er durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API Aufrufe, um AWS Resilience Hub über das Netzwerk darauf zuzugreifen. Clients müssen Transport Layer Security (TLS) 1.2 oder höher unterstützen. Wir empfehlen TLS 1.3 oder höher. Kunden müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie Ephemeral Diffie-Hellman () oder Elliptic Curve Ephemeral Diffie-Hellman (DHE) unterstützen. ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Resilienzprüfungen für AWS Dienste

Dieses Kapitel enthält Einzelheiten zu den verschiedenen Resilienzprüfungen, die von AWS Resilience Hub den unterstützten AWS Diensten durchgeführt werden, um sicherzustellen, dass die Ausfallsicherheit von Anwendungen nicht beeinträchtigt wird. Bei diesen Prüfungen werden das Wiederherstellungszeitziel (RTO) und das Wiederherstellungspunktziel (RPO) anhand der Werte geschätzt, die in der Ausfallsicherheitsrichtlinie für jede Anwendungskomponente (AppComponent) definiert sind. Die Bewertungen umfassen verschiedene Arten von Störungen, d. h. Anwendungs-, Infrastrukturausfälle, AZ-Ausfälle und regionale Ausfälle. Um diese Prüfungen durchführen zu können, müssen Sie jedoch die entsprechenden IAM Berechtigungen AWS Resilience Hub für den Zugriff auf Ihre Ressourcen bereitstellen. Weitere Informationen zu den erforderlichen IAM Berechtigungen für den AWS Resilience Hub Zugriff auf Ihre Ressourcen und die Durchführung der Resilienzprüfungen in diesem Kapitel finden Sie unterAWS verwaltete Richtlinien für AWS Resilience Hub.

AWS Dienste

- Amazon Elastic File System
- Amazon Relational Database Service und Amazon Aurora
- Amazon Simple Storage Service
- Amazon-DynamoDB
- Amazon Elastic Compute Cloud
- Amazon EBS
- AWS Lambda
- Amazon Elastic Kubernetes Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Elastic Container Service
- Elastic Load Balancing
- APIAmazon-Gateway
- Amazon DocumentDB
- NATGateway
- Amazon Route 53
- Amazon Route 53 Application Recovery-Controller

- Amazon FSx für Windows-Dateiserver
- AWS Step Functions

Amazon Elastic File System

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon Elastic File System gelten.

Weitere Informationen zu Amazon Elastic File System finden Sie in der Dokumentation zu Amazon Elastic File System.

Typ des Dateisystems

AWS Resilience Hub prüft den Dateisystemtyp: Regional oder One Zone. Der Dateisystemtyp wirkt sich auf die Widerstandsfähigkeit des Dateisystems bei Störungen der Infrastruktur oder des AZ-Bereichs aus. Weitere Informationen zu Dateisystemtypen finden Sie unter Verfügbarkeit und Haltbarkeit von EFS Amazon-Dateisystemen.

Dateisystem-Backup

AWS Resilience Hub prüft, ob ein AWS Backup Plan für das bereitgestellte Dateisystem definiert ist. Darüber hinaus wird überprüft, ob die `Cross-Region` Backup-Option aktiviert ist, um sicherzustellen, dass Störungen auf regionaler Ebene abgedeckt werden, falls dies in den Kundenrichtlinien vorgesehen ist.

Datenreplikation

AWS Resilience Hub prüft, ob eine regionsinterne oder regionsübergreifende EFS Amazon-Datenreplikation für das bereitgestellte Dateisystem definiert ist. Die EFS Amazon-Datenreplikation trägt dazu RPO bei, Schätzungen RTO und Schätzungen auf Anwendungs-, Infrastruktur-, AZ- und Regionsebene zu verbessern. AWS Resilience Hub Überprüft außerdem, ob sie mit einer In-Region kombiniert wird AWS Backup , um die Stabilität des Dateisystems bei Anwendungsunterbrechungen zu gewährleisten.

Amazon Relational Database Service und Amazon Aurora

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon Relational Database Service und Amazon Aurora gelten.

Weitere Informationen zu Amazon Relational Database Service und Amazon Aurora finden Sie in der Dokumentation zu Amazon Relational Database Service.

Single-AZ-Bereitstellung

AWS Resilience Hub prüft, ob die Datenbank als einzelne Instanz bereitgestellt wird, und wenn festgestellt wird, dass sie keine sekundäre Instanz und kein Read Replica unterstützt.

Multi-AZ-Bereitstellung

AWS Resilience Hub prüft, ob die Datenbank entweder mit einer sekundären Instanz oder mit Read Replicas bereitgestellt wird. Wenn die Datenbank mit Read Replica bereitgestellt wird, AWS Resilience Hub überprüft, ob sie in einer anderen AZ bereitgestellt wurde, um im Falle einer AZ-Unterbrechung ein Failover zu ermöglichen.

Backup

AWS Resilience Hub prüft, ob die folgenden Backup-Funktionen auf eine bereitgestellte Datenbankinstanz angewendet werden.

- AWS Backup Plan mit automatischer Backup-Option
- AWS Backup Plan mit regionsübergreifender Sicherungskopie, falls dies gemäß den Kundenrichtlinien erforderlich ist
- Manuelle Snapshots für Backup-Systeme von Drittanbietern

Regionsübergreifendes Failover

AWS Resilience Hub Kontrollen RTO und RPO Ziele, die in der Resilienzpolitik zur Wiederherstellung nach regionalen Störungen festgelegt sind. AWS Resilience Hub Kann außerdem folgende regionsübergreifende Architekturen identifizieren, um regionalen Störungen zu begegnen:

- Ein regionsinternes Backup mit einer Kopie eines regionsübergreifenden Snapshots
- Eine Read Replica in einer anderen Region
- Eine globale Amazon Aurora Aurora-Datenbank mit einem sekundären Cluster in einer anderen Region
- Eine globale Amazon Aurora Aurora-Datenbank mit einem kopflosen sekundären Cluster in einer anderen Region

Schnelleres Failover innerhalb der Region

AWS Resilience Hub Kontrollen RTO und RPO Ziele, die in der Ausfallsicherheitsrichtlinie bei Infrastruktur- oder AZ-Störungen definiert sind. AWS Resilience Hub Kann außerdem die folgenden regionalen Architekturen identifizieren, um Störungen bei Anwendungen, Infrastruktur und Verfügbarkeit abzudecken:

- Ein regionsinternes Backup
- Eine Read Replica in einer anderen AZ
- Ein Aurora-Cluster mit einer Read Replica in einer anderen AZ
- Eine Multi-AZ-Instance von Amazon Relational Database Service (Amazon) RDS
- Ein Amazon RDS Multi-AZ-Cluster
- Eine einzelne Instanz von Amazon RDS mit einer Read Replica in einer anderen AZ

Amazon Simple Storage Service

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon Simple Storage Service (Amazon S3) gelten.

Weitere Informationen zu Amazon S3 finden Sie in der Amazon S3 S3-Dokumentation.

Versionsverwaltung

AWS Resilience Hub überprüft, ob ein Amazon S3 S3-Bucket mit aktivierter Versionierung konfiguriert ist.

Geplantes Backup

AWS Resilience Hub prüft, ob ein AWS Backup Plan für den bereitgestellten Amazon Simple Storage Service (Amazon S3) -Bucket definiert ist. Darüber hinaus wird geprüft, ob die regionsübergreifende Backup-Option aktiviert ist, wenn Ihre Police den Schutz von Störungen auf regionaler Ebene vorsieht.

PC-Wiederherstellung oint-in-time

Datenreplikation

AWS Resilience Hub wenn für den bereitgestellten Amazon S3 S3-Bucket eine Replikation in derselben Region (SRRCRR) und eine regionsübergreifende Replikation () definiert ist.

Die Amazon S3 S3-Datenreplikation verbessert die geschätzte Arbeitslast RTO und die geschätzte Arbeitslast RPO auf Anwendungs-, Infrastruktur-, AZ- und Regionsebene. Darüber hinaus schützt es auch vor dem physischen Löschen von Objekten, da das Löschen einer Objektversion nicht in den Amazon S3 S3-Ziel-Bucket repliziert wird. AWS Resilience Hub Prüft außerdem auf der Grundlage der in Ihrer Ausfallsicherheitsrichtlinie definierten RTO Ziele, ob Amazon S3 Replication Time Control (S3RTC) aktiviert werden sollte oder nicht. Diese kostenpflichtige Funktion repliziert 99,99 Prozent der Quell-Bucket-Objekte innerhalb von 15 Minuten.

- AWS Backup Plan mit automatischer Backup-Option
- AWS Backup Plan mit regionsübergreifender Sicherungskopie, falls dies gemäß den Kundenrichtlinien erforderlich ist
- Manuelle Snapshots für Backup-Systeme von Drittanbietern

Amazon-DynamoDB

In diesem Abschnitt werden alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon DynamoDB gelten.

Weitere Informationen zu Amazon DynamoDB finden Sie in der Amazon DynamoDB DynamoDB-Dokumentation.

Geplante Sicherung

AWS Resilience Hub prüft, ob für die bereitgestellte Tabelle bereits ein Backup definiert ist. Darüber hinaus wird geprüft, ob ein regionsübergreifendes Backup für Ihre Police konfiguriert werden sollte, falls diese Deckung für Störungen auf regionaler Ebene erfordert.

PC-Wiederherstellung oint-in-time

AWS Resilience Hub prüft, ob point-in-time Recovery (PITR) gemäß dem Ziel Ihrer Resilienz-Richtlinie erforderlich istRPO. Regionsübergreifendes Backup wird jedoch nicht unterstützt für.

PITR Daher verwenden Sie einen vorhandenen geplanten AWS Backup Plan mit aktivierter regionsübergreifender Backup-Option oder erstellen einen neuen.

Globale Tabelle

Amazon Elastic Compute Cloud

In diesem Abschnitt werden alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon Elastic Compute Cloud gelten.

Weitere Informationen zu Amazon Elastic Compute Cloud finden Sie in der Dokumentation zu Amazon Elastic Compute Cloud.

Zustandsbehaftete Instanz

AWS Resilience Hub identifiziert eine EC2 Amazon-Instance als stateful-Instance, wenn eines der folgenden Kriterien erfüllt ist:

- Wenn `DeleteOnTermination` das Attribut für mindestens ein Amazon Elastic Block Store (AmazonEBS) -Volume, das an diese Instance angehängt ist, auf false gesetzt ist.
- Wenn Amazon Data Lifecycle Manager oder ein AWS Backup Plan an die EC2 Amazon-Instance oder mindestens ein EBS Amazon-Volume angehängt ist.
- AWS Elastic Disaster Recovery Es wird verwendet, um Ihre EC2 Amazon-Instance-Speichervolumen zu replizieren.

> **Note**
>
> Wenn eine EC2 Amazon-Instance keines der oben genannten Kriterien erfüllt, wird sie als statuslose EC2 Amazon-Instance AWS Resilience Hub behandelt.

Auto-Scaling-Gruppen

AWS Resilience Hub sucht nach einer Gruppe von statusfreien EC2 Amazon-Instances. Falls entdeckt, wird empfohlen, dasselbe mithilfe von Auto Scaling Scaling-Gruppen (ASG) mit Multi-AZ-Konfiguration zu orchestrieren.

Wenn ein vorhandenes Objekt identifiziert ASG wird, ARH wird überprüft, ob es für mehrere Availability Zones konfiguriert ist. Wenn auch definiert ASG ist, dass nur EC2 Spot-Amazon-Instances verwendet werden, wird empfohlen, die Kapazität durch EC2 On-Demand-Amazon-Instances zu erweitern, um die Ausfallsicherheit zu verbessern

wenn EC2 Spot-Amazon-Instances nicht verfügbar sind.

EC2Amazon-Flotte

AWS Resilience Hub identifiziert Amazon EC2 Fleet und überprüft, ob es sich um eine Multi-AZ-Bereitstellung handelt und ob nur EC2 Spot-Amazon-Instances verwendet werden.

Durch die Definition einer EC2 Amazon-Flotte als Multi-AZ-Bereitstellung wird ihre Widerstandsfähigkeit im Falle einer AZ-Störung verbessert.

Die Erweiterung einer EC2 Amazon-Flotte um On-Demand-Instances verbessert ihre Widerstandsfähigkeit, wenn Spot-Instances nicht verfügbar sind.

Amazon EBS

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon geltenEBS.

Weitere Informationen zu Amazon EBS finden Sie in der EBSAmazon-Dokumentation.

Geplantes Backup

AWS Resilience Hub prüft, ob eine oder beide der folgenden Optionen für Ihre EBS Amazon-Volumes definiert sind.

- Eine Backup-Regel für ein bestimmtes EBS Amazon-Volume, das an Ihre EC2 Amazon-Instance angehängt ist.
- Eine Backup-Regel zum Erstellen von EBS Amazon-Backups AMI auf Ihrer EC2 Amazon-Instance.
- Manuelle Snapshots für Backup-Systeme von Drittanbietern.

Wenn Ihre Police den Schutz von Störungen auf regionaler Ebene vorsieht, überprüfen Sie außerdem, ob in Ihrer Backup-Regel die AWS Resilience Hub Option regionsübergreifendes Backup aktiviert ist.

Datensicherung und Replikation

AWS Resilience Hub identifiziert, dass ein EBS Amazon-Volume als statusbehaftetes Volumen betrachtet wird, wenn eines der folgenden Kriterien erfüllt ist:

- Wenn `DeleteOnTermination` das Attribut für dieses EBS Amazon-Volume auf False gesetzt ist.
- Wenn Amazon Data Lifecycle Manager oder ein AWS Backup Plan entweder diesem EBS Amazon-Volume oder der EC2 Amazon-Instance zugeordnet ist, an die es angehängt ist.
- AWS Elastic Disaster Recovery Es wird verwendet, um Ihre EC2 Amazon-Instance-Speichervolumen zu replizieren.

AWS Lambda

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die spezifisch für AWS Lambda.

Weitere Informationen zu AWS Lambda finden Sie in der AWS Lambda Dokumentation.

Amazon VPC Access für Kunden

AWS Resilience Hub identifiziert eine AWS Lambda Funktion, die mit dem Kunden verbunden istVPC. Die Verbindung AWS Lambda zu Subnetzen in verschiedenen AZs Amazon-Ländern VPC ermöglicht die Funktionsstabilität im Falle einer AZ-Störung.

Warteschlange für unzustellbare Briefe

AWS Resilience Hub prüft, ob an eine AWS Lambda Funktion eine Warteschlange für unzustellbare Buchstaben (DLQ) angehängt ist, in der fehlgeschlagene Anfragen gespeichert werden können. Das Anhängen einer AWS Lambda Funktion DLQ an ermöglicht es, den Datenverlust von Anfragen zu verhindern und zu einem späteren Zeitpunkt erneut zu versuchen, die fehlgeschlagenen Anfragen zu verarbeiten.

Amazon Elastic Kubernetes Service

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon Elastic Kubernetes Service (AmazonEKS) gelten.

Weitere Informationen zu Amazon EKS finden Sie in der EKSAmazon-Dokumentation.

Multi-AZ-Bereitstellung

AWS Resilience Hub identifiziert, ob die Pod-Bereitstellung auf mehreren Worker-Knoten in mehreren ausgeführt wirdAZs.

Ein zusätzlicher EKS Amazon-Cluster in einer anderen Region ist erforderlich, wenn Ihre Resilienz-Richtlinie den Schutz bei regionalen Störungen vorsieht. Dieser zusätzliche EKS Amazon-Cluster ist auch für Pod-Bereitstellungen verifiziert, die auf mehrere Worker-Knoten in mehreren AZs verteilt sind.

Bereitstellung vs. ReplicaSet

AWS Resilience Hub prüft, ob Sie Pod-Objekte anstelle von Deployment verwenden ReplicaSets . Das Ersetzen ReplicaSets von Pod-Objekten bei der Bereitstellung vereinfacht die Pod-Updates auf eine neue Version der Software und beinhaltet weitere nützliche Funktionen.

Bereitstellung und Wartung.

AWS Resilience Hub prüft, ob die folgenden bewährten Methoden für die Bereitstellung verwendet werden:

- Verwendung von Pod Disruption Budget (PDB) — PDB Mit dieser Option kann die Verfügbarkeit verbessert werden, indem die Anzahl der Pods im Workload, die zu einem bestimmten Zeitpunkt unterbrochen werden können, begrenzt wird.
- Ersetzen von selbstverwalteten Knotengruppen durch von Amazon EKS verwaltete Knotengruppen — Dieser Ersatz vereinfacht die Aktualisierung von Worker-Node-Images während der Wartung.
- Unterstützung dynamischer Anfragen CPU und Speicheranforderungen pro Bereitstellung — Diese Anfragen helfen Kubernetes bei der Auswahl eines Nodes, der den Anforderungen eines Pods entspricht.
- Konfiguration von Verfügbarkeits- und Bereitschaftstests für alle Container — Die Konfiguration von Verfügbarkeitstests trägt dazu bei, die Resilienz zu verbessern, indem die nicht funktionierenden Pods neu gestartet werden. Durch die Konfiguration von Bereitschaftstests kann die Verfügbarkeit verbessert werden, indem der Datenverkehr von den stark frequentierten Pods abgelenkt wird.
- Konfiguration von Karpenter, Cluster Autoscaler oder AWS Fargate — Diese Konfigurationen ermöglichen es der Infrastruktur von Amazon EKS Cluster, zu wachsen und die Workload-Anforderungen zu erfüllen.

- Konfiguration von Horizontal Pod Autoscaler — Diese Konfiguration hilft Amazon EKS Cluster, die Arbeitslast automatisch zu skalieren, um den Anforderungen der Anforderungsverarbeitung gerecht zu werden.

Amazon Simple Notification Service

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon Simple Notification Service (AmazonSNS) gelten.

Weitere Informationen zu Amazon SNS finden Sie in der SNSAmazon-Dokumentation.

Thema: Abonnements

AWS Resilience Hub prüft, ob an Amazon SNS Topic mindestens ein Abonnement angehängt ist, um sicherzustellen, dass eingehende Nachrichten nicht verloren gehen.

Amazon Simple Queue Service

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon Simple Queue Service (AmazonSQS) gelten.

Weitere Informationen zu Amazon SQS finden Sie in der SQSAmazon-Dokumentation.

Warteschlange für unzustellbare Briefe

AWS Resilience Hub prüft, ob der SQS Amazon-Warteschlange eine DLQ zugewiesen ist, um Nachrichten zu verarbeiten, die nicht erfolgreich an Abonnenten zugestellt werden können.

Amazon Elastic Container Service

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon Elastic Container Service (AmazonECS) gelten.

Weitere Informationen zu Amazon ECS finden Sie in der ECSAmazon-Dokumentation.

Multi-AZ-Bereitstellung

AWS Resilience Hub prüft AZs je nach Amazon- oder AWS Fargate Starttyp, ob ECS Amazon-Aufgaben EC2 oder -Dienste in mehreren ausgeführt werden. Ein zusätzlicher ECS Amazon-Cluster

in einer anderen Region ist erforderlich, wenn Ihre Police eine Deckung für regionale Störungen benötigt. Der zusätzliche Cluster wurde auch für die Ausführung mehrerer Aufgaben oder Dienste verifiziertAZs.

Elastic Load Balancing

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die für Elastic Load Balancing spezifisch sind.

Weitere Informationen zu Elastic Load Balancing finden Sie in der Elastic Load Balancing Balancing-Dokumentation.

Multi-AZ-Bereitstellung

AWS Resilience Hub prüft, ob Elastic Load Balancing in mehreren ausgeführt wirdAZs.

Ein zusätzliches Elastic Load Balancing in einer anderen Region ist erforderlich, wenn Ihre Police eine Deckung für regionale Störungen benötigt. Das zusätzliche Elastic Load Balancing, das sich in einer anderen Region befindet, wurde ebenfalls für seinen Einsatz in mehreren Regionen verifiziertAZs.

APIAmazon-Gateway

In diesem Abschnitt sind alle Resilienzprüfungen und Empfehlungen aufgeführt, die speziell für Amazon API Gateway gelten.

Weitere Informationen zu Amazon API Gateway finden Sie in der Amazon API Gateway-Dokumentation.

Regionalübergreifender Einsatz

Wenn in Ihrer Richtlinie regionale Störungen berücksichtigt werden müssen, AWS Resilience Hub wird geprüft, ob eine zusätzliche Amazon API API Gateway-Ressource in einer anderen Region bereitgestellt wird.

Private API Multi-AZ-Bereitstellung

AWS Resilience Hub prüft, ob Ihr in Amazon API Gateway als privat definiert API ist. Private APIs sollte Datenverkehr über den VPC Amazon-Schnittstellenendpunkt empfangen, der für mehrere bereitgestellt wirdAZs.

Amazon DocumentDB

In diesem Abschnitt sind alle Prüfungen und Empfehlungen aufgeführt, die speziell für Amazon DocumentDB gelten.

Weitere Informationen zu Amazon DocumentDB finden Sie in der Amazon DocumentDB DocumentDB-Dokumentation.

Multi-AZ-Bereitstellung

AWS Resilience Hub prüft, ob der Amazon DocumentDB-Cluster in mehreren AZs bereitgestellt wird. Ein zusätzlicher sekundärer Amazon DocumentDB-Cluster ist in einer anderen Region erforderlich, wenn Ihre Police eine Deckung für regionale Störungen vorsieht. Der zusätzliche Amazon DocumentDB-Cluster, der sich in einer anderen Region befindet, wurde ebenfalls mehrfach AZs auf seine Ausführung überprüft.

Elastischer Cluster und Multi-AZ-Bereitstellung

AWS Resilience Hub prüft, ob Amazon DocumentDB Elastic Cluster-Shards Read Replicas verwenden, die in verschiedenen Umgebungen bereitgestellt werden. AZs

Elastischer Cluster und manuelle Snapshots

AWS Resilience Hub prüft, ob regelmäßig manuelle Snapshots für einen Amazon DocumentDB Elastic-Cluster erstellt werden. Manuelle Snapshots ermöglichen eine längere Persistenz und bieten Flexibilität bei der Festlegung der Snapshot-Häufigkeit, die Ihren Geschäftsanforderungen entspricht.

NATGateway

In diesem Abschnitt sind alle Prüfungen und Empfehlungen aufgeführt, die für NAT Gateway spezifisch sind. Weitere Informationen zu NAT Gateways finden Sie unter NATGateways.

Multi-AZ-Bereitstellung

AWS Resilience Hub prüft, ob NAT Gateway in mehreren bereitgestellt wird. AZs

Eine zusätzliche NAT Gateway-Bereitstellung ist in einer anderen Region erforderlich, wenn Ihre Police die Deckung regionaler Störungen vorsieht. Das zusätzliche NAT Gateway, das sich in einer anderen Region befindet, wurde ebenfalls auf seinen Einsatz in mehreren Regionen verifiziertAZs.

Amazon Route 53

In diesem Abschnitt sind alle Prüfungen und Empfehlungen aufgeführt, die speziell für Amazon Route 53 gelten.

Weitere Informationen zu Amazon Route 53 finden Sie in der Dokumentation zu Amazon Route 53.

Multi-AZ-Bereitstellung

AWS Resilience Hub prüft, ob der Datensatz für die gehostete Zone von Amazon Route 53 mit mehreren Zielen in derselben Region definiert ist und ob diese Ziele in mehreren bereitgestellt werdenAZs. Wenn Ihre Police eine Deckung für regionale Störungen vorsieht, AWS Resilience Hub prüft Sie, ob der Datensatz für die gehostete Zone von Amazon Route 53 in mehreren Regionen mit mehreren Zielen pro Region definiert ist und ob diese Ziele in mehreren bereitgestellt werdenAZs.

Amazon Route 53 Application Recovery-Controller

In diesem Abschnitt sind alle Prüfungen und Empfehlungen aufgeführt, die speziell für Amazon Route 53 Application Recovery Controller (Route 53ARC) gelten.

Weitere Informationen zu Route 53 ARC finden Sie in der ARCDokumentation zu Route 53

Multi-AZ-Bereitstellung

AWS Resilience Hub prüft, ob ähnliche Ressourcen in mehreren Regionen eingesetzt werden, und empfiehlt als bewährte Methode, ARC Route-53-Bereitschaftsprüfungen zu definieren, um deren Verfügbarkeit und Bereitschaft im Falle einer regionalen Störung zu erhöhen. Sie werden darüber informiert, dass zusätzliche Stundengebühren anfallen werden.

Amazon FSx für Windows-Dateiserver

In diesem Abschnitt sind alle Prüfungen und Empfehlungen aufgeführt, die speziell FSx für Amazon for Windows File Server gelten. Weitere Informationen zu Amazon FSx für Windows File Server finden Sie in der Dokumentation zu Amazon FSx for Windows File Server.

Typ des Dateisystems

AWS Resilience Hub prüft den Dateisystemtyp: `Regional` oder. `One Zone` Der Dateisystemtyp beeinträchtigt seine Widerstandsfähigkeit im Falle von Infrastruktur- oder AZ-Störungen. Weitere Informationen zu Dateisystemtypen finden Sie auf Amazon EFS.

Dateisystem-Backup

AWS Resilience Hub prüft, ob an für AWS Backup das bereitgestellte Dateisystem definiert ist. Außerdem wird geprüft, ob die `cross-Region backup` Option aktiviert ist, wenn Ihre Police die Deckung von Störungen auf regionaler Ebene vorsieht.

Datenreplikation

AWS Resilience Hub prüft, ob für das bereitgestellte Dateisystem eine geplante regionsinterne oder regionsübergreifende AWS DataSync Datenreplikationsaufgabe definiert ist.

AWS DataSync Eine geplante Datenreplikationsaufgabe kann die geschätzte Arbeitslast RTO und die geschätzte Arbeitslast RPO auf Infrastruktur-, AZ- und Regionsebene verbessern. Darüber hinaus könnte sie mit einer Lösung innerhalb der Region kombiniert werden AWS Backup , um die Daten im Fall einer Anwendungsunterbrechung wiederherzustellen.

AWS Step Functions

In diesem Abschnitt sind alle Prüfungen und Empfehlungen aufgeführt, die spezifisch für. AWS Step Functions

Weitere Informationen zu AWS Step Functions finden Sie in der AWS Step Functions Dokumentation.

Versionierung und Alias

AWS Resilience Hub prüft, ob der AWS Step Functions Workflow Versionierung und Alias verwendet, um die Zeit für die erneute Bereitstellung zu verkürzen.

Regionsübergreifender Einsatz

AWS Resilience Hub prüft, ob ein AWS Step Functions Workflow desselben Workflowtyps in einer anderen Region bereitgestellt wird, um ihn im Falle einer regionalen Störung wiederherzustellen.

Arbeiten mit anderen -Services

In diesem Abschnitt werden AWS Dienste beschrieben, die mit interagieren AWS Resilience Hub.

Themen

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

AWS CloudFormation

AWS Resilience Hub ist in AWS CloudFormation integriert, ein Service, der Ihnen hilft, Ihre AWS-Ressourcen zu modellieren und einzurichten, damit Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen können. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt (z. B. AWS::ResilienceHub:::ResiliencyPolicy und AWS::ResilienceHub:::App) und diese Ressourcen für Sie AWS CloudFormation bereitstellt und konfiguriert.

Wenn Sie AWS CloudFormation verwenden, können Sie Ihre Vorlage wiederverwenden, um Ihre AWS Resilience Hub-Ressourcen einheitlich und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen wiederholt in mehreren AWS Konten und Regionen bereit.

AWS Resilience Hub- und AWS CloudFormation-Vorlagen

Um Ressourcen für AWS Resilience Hub und verwandte Dienstleistungen bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation-Vorlagen kennen und verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer verwenden, der den Einstieg in die Arbeit mit AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

AWS Resilience Hubunterstützt das Erstellen AWS::ResilienceHub:::ResiliencyPolicy und AWS::ResilienceHub:::App Eingeben vonAWS CloudFormation. Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für AWS::ResilienceHub:::ResiliencyPolicy und

AWS::ResilienceHub:::App, finden Sie in der Referenz zum AWS Resilience Hub Ressourcentyp im AWS CloudFormationBenutzerhandbuch.

Sie können AWS CloudFormation Stacks verwenden, um Anwendungen zu definierenAWS Resilience Hub. Mit einem Stack können Sie verwandte Ressourcen als eine Einheit verwalten. Ein Stapel kann alle Ressourcen enthalten, die Sie zum Ausführen einer Webanwendung benötigen, z. B. einen Webserver oder Netzwerkregeln.

Weitere Informationen zu AWS CloudFormation

Weitere Informationen zu AWS CloudFormation finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation API Referenz
- AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle

AWS CloudTrail

AWS Resilience Hub ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in AWS Resilience Hub ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe AWS Resilience Hub als Ereignisse. Zu den aufgezeichneten Aufrufen gehören Aufrufe von der AWS Resilience Hub Konsole und Codeaufrufen für die AWS Resilience Hub API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Resilience Hub. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS Resilience Hub, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

AWS Systems Manager

AWS Resilience Hub arbeitet mit Systems Manager zusammen, um die Schritte Ihrer SOPs zu automatisieren, indem es eine Reihe von SSM-Dokumenten bereitstellt, die Sie als Grundlage für diese SOPs verwenden können.

AWS Resilience Hub stellt Ihnen AWS CloudFormation Vorlagen zur Verfügung, die die IAM-Rollen enthalten, die für die Ausführung verschiedener Systems Manager Manager-Dokumente erforderlich sind, eine Rolle pro Dokument mit den für das jeweilige Dokument erforderlichen Berechtigungen. Nach dem Erstellen eines Stacks mit der AWS CloudFormation Vorlage werden die IAM-Rollen eingerichtet und Metadaten im Systems Manager Manager-Parameter gespeichert, damit das Systems Manager Manager-Automatisierungsdokument für verschiedene Wiederherstellungsverfahren ausgeführt werden kann.

Weitere Informationen zur Verwendung von SOPs finden Sie unter. Verwaltung von Standardarbeitsanweisungen

AWS Trusted Advisor

AWS Trusted Advisor ist eine zentrale Sammlung von AWS Best-Practice-Empfehlungen, die Ihnen dabei helfen, Ihre Implementierung zu identifizieren, zu priorisieren und zu optimieren. AWS AWS Trusted Advisor untersucht Ihre AWS Umgebung und gibt dann Empfehlungen, indem überprüft wird, ob Möglichkeiten bestehen, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen. Diese Prüfungen sind je nach Zweck in mehrere Kategorien unterteilt. Weitere Informationen zu den verschiedenen Kategorien von AWS Trusted Advisor Check-ins finden Sie im AWS SupportBenutzerhandbuch.

AWS Trusted Advisor bietet mehrere allgemeine Empfehlungen zur Ausfallsicherheit durch Resilienzprüfungen für jede Anwendung in der AWS Resilience Hub Kategorie Fehlertoleranz. In der Kategorie Fehlertoleranz sind alle Prüfungen aufgeführt, mit denen Ihre Anwendungen auf ihre Belastbarkeit und Zuverlässigkeit getestet werden. Mit diesen Prüfungen werden Sie bei AppComponent Ausfällen und Richtlinienverstößen gewarnt, die zu Ausfallrisiken führen und die Verfügbarkeit von Anwendungen zur Gewährleistung der Geschäftskontinuität beeinträchtigen können. Im Abschnitt „Empfohlene Maßnahmen“, auf den näher eingegangen werden muss, finden Sie außerdem Empfehlungen zur Ausfallsicherheit, mit denen Sie die Chancen zur Verringerung dieser Risiken verbessern können. AWS Resilience Hub Für weitere Informationen zu den Empfehlungen für die einzelnen Anwendungen in der empfehlen wir Ihnen AWS Trusted Advisor, die detaillierten Empfehlungen in der AWS Resilience Hub zu lesen.

AWS Trusted Advisor bietet die folgenden Prüfungen für jede Anwendung in AWS Resilience Hub:

- AWS Resilience Hub Bewertungen der Ausfallsicherheit von Anwendungen — Überprüft die Resilienzbewertung Ihrer Anwendungen anhand der letzten Bewertung von AWS Resilience Hub und warnt Sie, wenn die Resilienzwerte unter einem bestimmten Wert liegen.

Kriterien für Warnmeldungen

- Grün — Zeigt an, dass Ihre Anwendung einen Resilienzwert von 70 und höher hat.
- Gelb — Zeigt an, dass Ihre Anwendung einen Resilienzwert zwischen 40 und 69 aufweist.
- Rot — Zeigt an, dass Ihre Anwendung einen Resilienzwert von weniger als 40 hat.

Empfohlene Maßnahme

Um die Ausfallsicherheit zu verbessern und den bestmöglichen Stabilitätswert für Ihre Anwendung zu erzielen, führen Sie eine Bewertung mit der zuletzt aktualisierten Version Ihrer Anwendungsressourcen durch und implementieren Sie gegebenenfalls die empfohlenen Betriebsempfehlungen. Weitere Informationen zum Durchführen, Überprüfen und Implementieren von Bewertungen, zum Prüfen und Einbeziehen bzw. Ausschließen betrieblicher Empfehlungen und deren Umsetzung finden Sie unter den folgenden Themen:

- the section called “Durchführung von Resilienzbewertungen”
- the section called “Überprüfung der Bewertungsberichte”
- the section called “Überprüfung der Empfehlungen zur Ausfallsicherheit”
- the section called “Einschließlich oder ohne betriebliche Empfehlungen”

- AWS Resilience Hub Verletzung der Anwendungsrichtlinie — Überprüft, ob die AWS Resilience Hub Anwendungen die RTO- und RPO-Ziele erfüllen, die Sie für eine Anwendung festgelegt haben, und warnt Sie, wenn die Anwendung die RTO- und RPO-Ziele nicht erfüllt.

  Warnungskriterien

  - Grün — Zeigt an, dass die Anwendung über eine Richtlinie verfügt und dass der geschätzte Workload-RTO und der geschätzte Workload-RPO den RTO- und RPO-Zielen entsprechen.
  - Gelb — Zeigt an, dass die Anwendung über eine Richtlinie verfügt und nicht bewertet wurde.
  - Rot — Zeigt an, dass die Anwendung über eine Richtlinie verfügt und dass der geschätzte Workload-RTO und der geschätzte Workload-RPO die RTO- und RPO-Ziele nicht erfüllen.

  Empfohlene Maßnahme

  Um sicherzustellen, dass das geschätzte Workload-RTO und das geschätzte Workload-RPO Ihrer Anwendung immer noch den definierten RTO- und RPO-Zielen entsprechen, führen Sie regelmäßig Bewertungen mit der zuletzt aktualisierten Version Ihrer Anwendungsressourcen durch. Wenn Sie sicherstellen möchten, dass die Ausfallsicherheitsrichtlinie Ihrer Anwendung nicht verletzt wird, empfehlen wir Ihnen außerdem, den Bewertungsbericht zu lesen und die

empfohlenen Resilienzempfehlungen umzusetzen. Weitere Informationen AWS Resilience Hub zur Aktivierung der täglichen Durchführung von Bewertungen in Ihrem Namen, zur Durchführung von Bewertungen, zur Überprüfung der Resilienzempfehlungen und deren Umsetzung finden Sie in den folgenden Themen:

- the section called “Anwendungsressourcen bearbeiten”(Um die täglichen Tests in Ihrem Namen durchführen AWS Resilience Hub zu können, gehen Sie wie unter So bearbeiten Sie die Einstellungen für abweichende Benachrichtigungen Ihres Anwendungsverfahrens vor und aktivieren Sie das Kontrollkästchen Automatisch täglich bewerten.)
- the section called “Durchführung von Resilienzbewertungen”
- the section called “Überprüfung der Bewertungsberichte”
- the section called “Überprüfung der Empfehlungen zur Ausfallsicherheit”
- the section called “Einschließlich oder ohne betriebliche Empfehlungen”

- AWS Resilience Hub Alter der Bewerbungsbeurteilung — Prüft, wann Sie für jede Ihrer Bewerbungen zum letzten Mal eine Prüfung durchgeführt haben AWS Resilience Hub. Sie erhalten eine Benachrichtigung, wenn Sie innerhalb der angegebenen Anzahl von Tagen keine Prüfung durchgeführt haben.

  Kriterien für Warnmeldungen

  - Grün — Zeigt an, dass Sie in den letzten 30 Tagen eine Bewertung für Ihre Anwendung durchgeführt haben.
  - Gelb — Zeigt an, dass Sie in den letzten 30 Tagen keine Prüfung für Ihre Anwendung durchgeführt haben.

  Empfohlene Maßnahme

  Führen Sie regelmäßig Bewertungen durch, um die Ausfallsicherheit Ihrer Anwendungen zu verwalten und zu verbessern AWS. Wenn Sie Ihre Anwendung täglich in Ihrem Namen bewerten AWS Resilience Hub möchten, können Sie dies aktivieren, indem Sie in der AWS Resilience Hub Drift-Benachrichtigung das Kontrollkästchen Diese Anwendung täglich automatisch bewerten aktivieren. Um das Kontrollkästchen Diese Bewerbung täglich automatisch prüfen zu aktivieren, füllen Sie das Verfahren zur Änderung der Bewerbungsmitteilung unter Bearbeiten aus???.

  > **Note**
  >
  > Bei AWS Resilience Hub dieser Prüfung wird das Beurteilungsalter nur für Bewerbungen bestimmt, die mindestens einmal geprüft wurden.

- AWS Resilience Hub Prüfung der Anwendungskomponenten — Prüft, ob eine Anwendungskomponente (AppComponent) in Ihrer Anwendung nicht wiederhergestellt werden kann. Das heißt, wenn sie im Falle einer Unterbrechung AppComponent nicht wiederhergestellt wird, kann es zu unbekanntem Datenverlust und Systemausfällen kommen. Wenn die Warnkriterien auf Rot gesetzt sind, bedeutet dies, dass das nicht AppComponent wiederhergestellt werden kann.

  Empfohlene Maßnahme

  Um sicherzustellen, dass Ihr Gerät wiederherstellbar AppComponent ist, überprüfen und implementieren Sie die Resilienzempfehlungen und führen Sie dann eine neue Bewertung durch. Weitere Informationen zur Überprüfung der Resilienzempfehlungen finden Sie unter. the section called “Überprüfung der Empfehlungen zur Ausfallsicherheit”

Weitere Informationen zur Verwendung AWS Trusted Advisor finden Sie im AWS Support Benutzerhandbuch.

Dokumentenverlauf für das AWS Resilience Hub Benutzerhandbuch

In der folgenden Tabelle wird die Dokumentation für diese Version von beschrieben. AWS Resilience Hub

- APIVersion: neueste
- Letzte Aktualisierung der Dokumentation: 01. August 2024

Änderung	Beschreibung	Datum
AWS Resilience Hub führt Empfehlungen zur Gruppierung ein	AWS Resilience Hub führt eine neue intelligente Gruppierungsoption ein, mit der Ressourcen beim Onboarding Ihrer Anwendungen in Anwendungskomponenten (AppComponents) gruppiert werden können. Wenn Sie Resilienzanalysen durchführen, ist es wichtig AWS Resilience Hub, dass Ihre Ressourcen genau in die richtigen Gruppen eingeteilt werden, um optimale und umsetzbare AppComponents Empfehlungen zu erhalten. Diese Option ist ideal für komplexe oder regionsübergreifende Anwendungen, um den Zeitaufwand für das Onboarding Ihrer Anwendungen zu reduzieren, und sie ergänzt den bestehenden Workflow für das Onboarding	1. August 2024

von Anwendungen, der heute verfügbar ist.

Weitere Informationen finden Sie unter den folgenden Themen:

- the section called “Verwaltung von Anwendungskomponenten”
- the section called “AWS Resilience Hub Empfehlungen zur Gruppierung von Ressourcen”

AWS Resilience Hub führt ein neues Widget mit einer Zusammenfassung der Bewertung ein	AWS Resilience Hub führt ein neues Widget mit Bewertungszusammenfassungen ein, das die generativen KI-Funktionen von Amazon Bedrock nutzt, um komplexe Resilienzdaten in umsetzbare Erkenntnisse umzuwandeln. In diesen Zusammenfassungen der Bewertungen werden die wichtigsten Ergebnisse extrahiert, Risiken priorisiert und Maßnahmen zur Verbesserung der Widerstandsfähigkeit empfohlen. Wenn Sie sich auf die wichtigsten Elemente konzentrieren, können Sie die Bewertungen viel leichter verstehen. So erhalten Sie aussagekräftige Informationen, die sich auf die wichtigsten Elemente Ihrer Resilienzsituation konzentrieren. Weitere Informationen finden Sie unter the section called “Zusammenfassung der Bewertung”.	1. August 2024

AWS Resilience Hub erweitert die Unterstützung für Amazon DocumentDB	Mit dieser AWS Resilienc e Hub Richtlinie können Sie `Describe` Berechtig ungen für den Zugriff auf Ressourcen und Konfigura tionen in Amazon DocumentD B, Elastic Load Balancing und AWS Lambda während der Durchführung von Bewertung en gewähren. Weitere Informationen zur AWS verwalteten Richtlinie finden Sie unterthe section called “AWSResilienceHubA sssessmentExecutionPolicy”.	1. August 2024

AWS Resilience Hub erweitert die Funktionen zur Erkennung von Abweichungen bei der Widerstandsfähigkeit von Anwendungen	AWS Resilience Hub hat seine Fähigkeiten zur Drifterkennung um eine neue Art der Drifterkennung erweitert: die Drift von Anwendungsressourcen. Diese Erweiterung erkennt Änderungen, wie z. B. das Hinzufügen oder Löschen von Ressourcen in den Eingabequellen der Anwendung. Sie können die Dienste „ AWS Resilience Hub Geplante Bewertung“ und „Benachrichtigung über Abweichungen“ aktivieren und sich benachrichtigen lassen, wenn eine Abweichung auftritt. Bei der letzten Resilienzbewertung wurden die Abweichungen identifiziert und es werden Abhilfemaßnahmen vorgestellt, damit die Anwendung wieder Ihren Ausfallsicherheitsrichtlinien entspricht. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Erkennung von Abweichungen” • the section called “Schritt 5: Richten Sie eine geplante Bewertung und eine Drift-Benachrichtigung ein”	8. Mai 2024

AWS Trusted Advisor Verbesserungen	AWS Resilience Hub hat die Unterstützung für erweitert, AWS Trusted Advisor indem eine Prüfung hinzugefü gt wurde, um Anwendung skomponenten zu identifiz ieren, die nicht wiederher gestellt werden können (). AppComponents Weitere Informationen finden Sie unter the section called “AWS Trusted Advisor”.	28. März 2024
AWS Resilience Hub erweitert die Unterstützung für empfohlene Alarme	AWS Resilience Hub hat die `README.md` Vorlagend atei mit Werten aktualisi ert, mit denen Sie Alarme erstellen können, die von AWS Resilience Hub intern AWS (z. B. Amazon CloudWatch) oder extern empfohlen werden AWS. Weitere Informationen finden Sie unter the section called “Verwalten von Alarmen”.	26. März 2024

AWS Resilience Hub erweitert die Unterstützung für Amazon FSx for Windows File Server	AWS Resilience Hub erweitert die Bewertungsunterstützung für Amazon FSx for Windows File Server-Ressourcen und bewertet gleichzeitig die Ausfallsicherheit Ihrer Anwendung. AWS Resilience Hub Bietet für Anwendungen, die Amazon FSx for Windows File Server verwenden, eine Reihe neuer Empfehlungen zur Ausfallsicherheit, die Availability Zone (AZ) und Multi-AZ-Bereitstellungen sowie Sicherungspläne sowie Datenreplikation abdecken. AWS Resilience Hub unterstützt Amazon FSx for Windows File Server, einschließlich der Dateisystemabhängigkeit von Microsoft Active Directory, sowohl für regionsinterne als auch für regionsübergreifende Bereitstellungen. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Unterstützte AWS Resilience Hub Ressourcen” • the section called “AWSResilienceHubAssessmentExecutionPolicy”	26. März 2024

	• the section called “Gruppieren von Ressourcen in einer Anwendungskomponente”	
AWS Resilience Hub bietet zusätzliche Informationen zum Resiliency Score	AWS Resilience Hub hat die Benutzererfahrung mit dem Resiliency Score aktualisiert, sodass Sie sich leichter zurechtfinden und verstehen können, welche Maßnahmen zur Verbesserung der Ausfallsicherheit Ihrer Anwendungen erforderlich sind. Weitere Informationen finden Sie unter the section called “Resilienzwerte verstehen”.	9. November 2023
AWS Resilience Hub erweitert die Unterstützung für Anwendungen, die Amazon Elastic Kubernetes Service (AmazonEKS) -Ressourcen enthalten	AWS Resilience Hub erweitert die Unterstützung für Anwendungen, die EKS Amazon-Ressourcen enthalten, um neue Betriebsempfehlungen. Bei der Durchführung einer Bewertung, die Ressourcen aus EKS Amazon-Clustern einbezieht, empfehlen wir nun, Tests und Alarme durchzuführen, um die Ausfallsicherheit der Anwendungen zu verbessern. Weitere Informationen finden Sie unter the section called “Verwaltung von Amazon Fault Injection Service-Experimenten”.	9. November 2023

AWS Resilience Hub bietet zusätzliche Informationen auf Anwendungsebene	AWS Resilience Hub stellt auf Anwendungsebene zusätzliche Informationen zur geschätzten Arbeitslast RTO und zur geschätzten Arbeitslast bereitRPO. Diese zusätzlichen Informationen geben Auskunft über die geschätzte maximale Arbeitslast RTO und die geschätzte Arbeitslast RPO Ihrer Anwendung aus der letzten erfolgreichen Bewertung. Bei diesem Wert handelt es sich um die geschätzte maximale Arbeitslast RTO und die geschätzte Arbeitslast RPO aller Arten von Störungen. Weitere Informationen finden Sie unter the section called “Verwalten von Anwendungen”.	30. Oktober 2023

AWS Resilience Hub erweitert die Bewertungsunterstützung für AWS Step Functions Ressourcen	AWS Resilience Hub erweitert die Bewertungsunterstützung für AWS Step Functions Ressourcen und bewertet gleichzeitig die Widerstandsfähigkeit Ihrer Anwendung. AWS Resilience Hub analysiert die AWS Step Functions Konfiguration einschließlich des Zustandsmaschinentyps (entweder Standard- oder Express-Workflows). Darüber hinaus gibt AWS Resilience Hub es Empfehlungen, die Ihnen helfen, die geschätzten Ziele für die Wiederherstellung der Arbeitslast (RTO) und die geschätzten Ziele für die Wiederherstellung des Workloads (RPO) zu erreichen. Um die Anwendungen einschließlich der AWS Step Functions Ressourcen bewerten zu können, müssen Sie die erforderlichen Berechtigungen einrichten, indem Sie entweder eine AWS verwaltete Richtlinie verwenden oder indem Sie die spezifische Berechtigung AWS Resilience Hub zum Lesen der AWS Step Functions Konfiguration manuell hinzufügen. Weitere Informationen zu den zugehörigen Berechtigungen	30. Oktober 2023

finden Sie unterthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

AWS Resilience Hub ermöglicht das Ausschließen von Betriebsempfehlungen	AWS Resilience Hub bietet Ihnen die Möglichkeit, Betriebsempfehlungen wie Alarme, Standardarbeitsanweisungen (SOPs) und Amazon Fault Injection Service (AWS FIS) -Tests auszuschließen. Während der Durchführung einer Bewertung erhalten Sie geschätzte Wiederherstellungszeiten und Empfehlungen AWS Resilience Hub, wie Sie die Ausfallsicherheit der bewerteten Anwendung erhöhen können. Mithilfe des Workflows zum Ausschließen von Empfehlungen haben Sie nun die Möglichkeit, empfohlene Alarme und AWS FIS TestsSOPs, die für sie nicht relevant sind, auszuschließen. Der Workflow zum Ausschließen ist von Vorteil, wenn Sie eine andere Plattform als die vorgeschlagene verwenden oder die Empfehlung bereits in einer alternativen Methode implementiert haben. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Einschließlich oder ohne betriebliche Empfehlungen”	9. August 2023

	• the section called “Einschränkung der Berechtigungen zum Ein- oder Ausschließen von AWS Resilience Hub Empfehlungen”	
Verbesserung des Berechtigungsdesigns für AWS Resilience Hub	AWS Resilience Hub führt ein neues Berechtigungsdesign ein, das Flexibilität bei der Konfiguration von AWS Identity and Access Management (IAM) -Rollen für bietet AWS Resilience Hub. Außerdem werden Berechtigungen in einer einzigen Rolle zusammengefasst, sodass benutzerdefinierte Rollennamen erstellt werden können, die für Sie und Ihre Teams von Bedeutung sind. Eine neue verwaltete Richtlinie ermöglicht es AWS Resilience Hub Ihnen, über die entsprechenden Berechtigungen für die unterstützten Dienste zu verfügen. Wenn Sie mit der aktuellen Methode zur Festlegung von Berechtigungen vertraut sind, werden wir die manuelle Konfiguration weiterhin unterstützen. Weitere Informationen zur AWS verwalteten Richtlinie finden Sie unterthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.	02. August 2023

Erkennung von Abweichungen bei der Ausfallsicherheit von Anwendungen mit AWS Resilience Hub	AWS Resilience Hub ermöglicht es Ihnen, proaktiv die notwendigen Maßnahmen zur Verbesserung der Ausfallsicherheit von Anwendungen zu erkennen und zu verstehen . Aktivierung von Amazon Simple Notification Service (AmazonSNS), Benachrichtigungen zu erhalten, wenn das geschätzte Ziel für die Workload-Wiederherstellungszeit (RTO) oder das geschätzte Ziel für den Workload-Wiederherstellungspunkt (RPO) vom Erreichen des Ziels auf das Erreichen der Geschäftsziele Ihres Unternehmens übergegangen ist. Wenn Sie von der reaktiven Identifizierung von Problemen mit der Ausfallsicherheit bei der manuellen Durchführung einer Bewertung zur proaktiven Benachrichtigung über SNS Amazon-Themen übergehen, können Sie potenzielle Störungen früher antizipieren und zusätzliche Sicherheit schaffen, dass die Wiederherstellungsziele erreicht werden. Weitere Informationen finden Sie unter den folgenden Themen:	02. August 2023

- the section called “Schritt 5: Richten Sie eine geplante Bewertung und eine Drift-Benachrichtigung ein”
- the section called “Anwendungsressourcen bearbeiten”

AWS Resilience Hub verbessert die Unterstützung für Amazon Relational Database Service und Amazon Aurora	AWS Resilience Hub erweitert die Bewertungsunterstützung für Amazon Relational Database Service Proxy- und Headless- und Amazon Aurora DB-Datenbankkonfigurationen. Darüber hinaus werden wir bei der Bewertung von Anwendungen, die Amazon beinhaltenRDS, nun zwischen verschiedenen Datenbank-Engines unterscheiden, um genauere geschätzte Ziele für die Workload-Wiederherstellungszeit zu erhalten (RTOs). AWS Resilience Hub bietet außerdem zusätzliche Maßnahmen zur Implementierung von Best Practices für Resilienz in Ihrer AWS Umgebung. Zu den Best Practices können Leistungseinblicke mit DevOps Guru für AmazonRDS, verbesserte Überwachung und automatische Bereitstellung auf unterstützten Datenbank-Engines gehören. Weitere Informationen zu den Berechtigungen, die erforderlich sind AWS Resilience Hub , um Ressourcen aus allen unterstützten Diensten in Ihre Bewertung einzubeziehen, finden Sie unterthe section	02. August 2023

	called “AWSResilienceHubAsssessmentExecutionPolicy”.	
AWS Resilience Hub erweitert die Unterstützung für Amazon Elastic Block Store-Snapshots	AWS Resilience Hub erweitert die Bewertungsunterstützung für Amazon Elastic Block Store (AmazonEBS), um EBS Amazon-Snapshots zu erkennen, die innerhalb derselben EBS Amazon-Region mit Direct APIs aufgenommen wurden. Der erweiterte Support gilt zusätzlich zum aktuellen Support für Kunden, die Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) oder AWS Backup verwenden. Weitere Informationen finden Sie unter Amazon Elastic Block Store (AmazonEBS).	02. August 2023

Verbesserungen von Amazon Elastic Compute Cloud	AWS Resilience Hub hat die Unterstützung für Amazon Elastic Compute Cloud (AmazonEC2) erweitert. AWS Ermöglicht seinen Kunden, die Amazon EC2 verwenden , die für ihren Anwendung sfall geeignete Konfiguration für Anwendungen unterschi edlicher Größe auszuwähl en. AWS Resilience Hub unterstützt die Bewertung der folgenden EC2 Amazon-Ko nfigurationen: • On-Demand-Instances. • Instanzen werden von AWS Backup und nach gesichert AWS Elastic Disaster Recovery. • Support für auto-scaling skalierende Gruppen mit Amazon Route 53 Applicati on Recovery Controller (Route 53ARC) In Zukunft wird sich der Assessment-Support auf Spot-Instances, Dedicated Hosts, Dedicated Instances , Placement-Gruppen und Flotten ausweiten. Weitere Informationen finden Sie unter the section called “AWS Resilience Hub	27. Juni 2023

	Referenz zu Zugriffsberechtigungen”.	
AWS verwaltete Richtlinienaktualisierungen	Es wurde eine neue Richtlinie hinzugefügt, die den Zugriff auf andere AWS Dienste für die Durchführung von Bewertungen ermöglicht. Weitere Informationen finden Sie unter the section called “AWSResilienceHubAsssessmentExecutionPolicy”.	26. Juni 2023
Neue Amazon DynamoDB DynamoDB-Alarme für Betriebsempfehlungen	Für Anwendungen, die Amazon DynamoDB verwenden, steht AWS Resilience Hub jetzt eine neue Reihe von Alarmen zur Verfügung, die Sie vor Ausfallrisiken für On-Demand-Kapazitätsmodi und bereitgestellte Kapazitätsmodi und globale Tabellen warnen. Um auf die neuen Alarme zugreifen zu können, müssen Sie möglicherweise die Richtlinie AWS Identity and Access Management (IAM) der Rolle aktualisieren, die Sie verwenden. Weitere Informationen finden Sie unter the section called “AWS Resilience Hub Referenz zu Zugriffsberechtigungen”.	2. Mai 2023

AWS Trusted Advisor Verbesserungen	AWS Resilience Hub hat die Unterstützung für AWS Trusted Advisor und die Anwendungen, die Amazon DynamoDB verwenden , erweitert. Wenn Sie AWS Trusted Advisor mit verwenden AWS Resilienc e Hub, können Sie jetzt eine Benachrichtigung erhalten, wenn ein Antrag in den letzten 30 Tagen nicht geprüft wurde. In dieser Benachrichtigung werden Sie aufgefordert, die Anwendung erneut zu bewerten, um festzustellen, ob es Änderungen gibt, die sich auf die Widerstandsfähigke it der Anwendung auswirken würden. Weitere Informationen zur AWS Resilience Hub Altersprü fung bei der Bewertung finden Sie unter. the section called “AWS Trusted Advisor”	2. Mai 2023

Zusätzliche Unterstützung für Amazon Simple Storage Service	Zusätzlich zur aktuellen Unterstützung von Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (Amazon S3CRR)/ Amazon S3 Same-Region Replication (SRR), Versionierung und AWS Backup AWS Resilience Hub wird Amazon S3 nun auch für die Konfiguration von Access Point für mehrere Regionen, Amazon S3 Replication Time Control (Amazon S3RTC) und AWS Backup point-in-time Recovery () geprüft. PITR Weitere Informationen finden Sie unter den folgenden Themen: • the section called “AWS Resilience Hub Referenz zu Zugriffsberechtigungen” • Verwaltung Ihres Amazon S3 S3-Speichers	21. März 2023

Zusätzliche Unterstützung für Amazon Elastic Kubernetes Service	AWS Resilience Hub hat EKS Amazon-Cluster als unterstützte Ressource für die Definition, Validierung und Nachverfolgung der Ausfallsicherheit von Anwendungen hinzugefügt. Kunden können EKS Amazon-Cluster zu neuen oder bestehenden Anwendungen hinzufügen und Bewertungen und Empfehlungen zur Verbesserung der Ausfallsicherheit erhalten. Kunden können Anwendungsressourcen mithilfe von Terraform AWS CloudFormation, AWS Resource Groups und hinzufügen. AppRegistry Darüber hinaus können Kunden einen oder mehrere EKS Amazon-Cluster direkt in einer oder mehreren Regionen mit einem oder mehreren Namespaces in jedem Cluster hinzufügen. Dies ermöglicht AWS Resilience Hub die Bereitstellung einzelner und regionsübergreifender Bewertungen und Empfehlungen. Replicas und Pods werden nicht nur die Bereitstellungen untersuchen ReplicationControllers, sondern auch die allgemeine AWS Resilience Hub Ausfallsicherheit des Clusters analysieren. AWS	21. März 2023

Resilience Hub unterstützt statuslose EKS Amazon-Cl uster-Workloads. Die neuen Funktionen sind in allen AWS Regionen verfügbar, in denen sie unterstützt AWS Resilience Hub werden.

Weitere Informationen finden Sie unter den folgenden Themen:

- the section called “Schritt 2: Verwalten Sie Ihre Anwendungsressourcen”
- the section called “Fügen Sie Cluster hinzu EKS”
- the section called “AWS Resilience Hub Referenz zu Zugriffsberechtigungen”
- AWS Regionale Dienste

Zusätzliche Unterstützung für Amazon Elastic File System	Zusätzlich zur aktuellen Unterstützung für Amazon Elastic File System (AmazonEFS) -Backups AWS Resilience Hub wird Amazon nun auch im Hinblick auf EFS EFS Amazon-Replikation und AZ-Konfiguration geprüft. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Unterstützte AWS Resilience Hub Ressourcen” • Was ist Amazon Elastic File System?	21. März 2023
Support für Anwendung seingabequellen	AWS Resilience Hub bietet jetzt Transparenz über Ihre Anwendungsquellen. Es hilft Ihnen, Eingabequellen Ihrer Anwendung hinzuzufügen, zu löschen und erneut zu importieren und eine neue Anwendungsversion zu veröffentlichen. Weitere Informationen finden Sie unter the section called “Anwendungsressourcen bearbeiten”.	21. Februar 2023

Support für Anwendungskonfigurationsparameter	AWS Resilience Hub bietet jetzt einen Eingabemechanismus, um zusätzliche Informationen über die Ressourcen zu sammeln, die Ihren Anwendungen zugeordnet sind. Anhand dieser Informationen AWS Resilience Hub erhalten Sie ein tieferes Verständnis Ihrer Ressourcen und können Ihnen bessere Empfehlungen zur Ausfallsicherheit geben. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Konfigurationsparameter der Anwendung” • the section called “Schritt 7: Konfigurieren Sie die Konfigurationsparameter der Anwendung” • the section called “Die Konfigurationsparameter der Anwendung werden aktualisiert”	21. Februar 2023

Zusätzliche Unterstützung für Amazon Elastic Block Store	Zusätzlich zur aktuellen Unterstützung von Amazon Elastic Block Store (AmazonEBS) -Volumes AWS Resilience Hub werden EBS Amazon-Snapshots nun anhand von Amazon Data Lifecycle Manager und Amazon EBS Fast Snapshot Restore (FSR) bewertet. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “AWS Resilience Hub Referenz zu Zugriffsberechtigungen” • Amazon Elastic Block Store (AmazonEBS)	21. Februar 2023

Integration mit AWS Trusted Advisor	AWS Trusted Advisor Benutzer können die mit ihrem Konto verknüpften Anwendungen einsehen, die von bewertet wurden AWS Resilience Hub. AWS Trusted Advisor zeigt den aktuellen Resilienzwert an und gibt einen Status an, der angibt, ob die angestrebte Resilienzpolitik (RTOundRPO) erfüllt wurde oder nicht. Jedes Mal, wenn eine Bewertung durchgeführt wird, wird sie AWS Trusted Advisor mit den neuesten Ergebnissen AWS Resilience Hub aktualisiert. AWS Trusted Advisor ist ein Service, der Ihre AWS Konten kontinuierlich analysiert und Empfehlungen gibt, die Ihnen helfen, AWS bewährte Verfahren und AWS Well-Architected-Richtlinien zu befolgen. Weitere Informationen finden Sie unter the section called “AWS Trusted Advisor”.	18. November 2022

Support für Amazon Simple Notification Service (AmazonSNS)	AWS Resilience Hub bewertet jetzt Anwendungen, die Amazon verwenden, SNS indem die SNS Amazon-Konfiguration, einschließlich der Abonnenten, analysiert wird, und gibt Empfehlungen zur Erreichung der geschätzten Workload-Wiederherstellungsziele des Unternehmens (geschätzte Arbeitslast RTO und geschätzte Arbeitslast RPO) für die Anwendungen. Amazon SNS ist ein verwalteter Service, der Nachrichten von Verlagen (Produzenten) an Abonnenten (Verbraucher) übermittelt. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Unterstützte AWS Resilience Hub Ressourcen” • the section called “Identitäts- und Zugriffsverwaltung” • the section called “Gruppieren von Ressourcen in einer Anwendungskomponente”	16. November 2022

Zusätzliche Support für Amazon Route 53 Application Recovery Controller (Amazon Route 53ARC)	AWS Resilience Hub bewertet jetzt Amazon Route 53 ARC im Hinblick auf Elastic Load Balancing und Amazon Relational Database Service (AmazonRDS). Dazu gehört auch die Beratung, wann Amazon Route 53 von Vorteil ARC wäre. Erweiterung AWS Resilience Hub der Amazon Route ARC 53-Assessment-Unterstützung über AWS Auto Scaling Group (AWS ASG) und Amazon DynamoDB hinaus. Amazon Route 53 ARC bietet Hochverfügbarkeit für Ihre Anwendung, sodass Sie schnell ein Failover Ihrer gesamten Anwendung in eine Failover-Region durchführen können. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Unterstützte AWS Resilience Hub Ressourcen” • the section called “Identitäts- und Zugriffsverwaltung”	16. November 2022

Zusätzliche Support für AWS Backup	AWS Resilience Hub bewertet jetzt Amazon Route 53 ARC im Hinblick auf Elastic Load Balancing und Amazon Relational Database Service (AmazonRDS). Dazu gehört auch die Beratung, wann Amazon Route 53 von Vorteil ARC wäre. Erweiterung AWS Resilience Hub der Amazon Route ARC 53-Assessment-Unterstützung über AWS Auto Scaling Group (AWS ASG) und Amazon DynamoDB hinaus. Amazon Route 53 ARC bietet Hochverfügbarkeit für Ihre Anwendung, sodass Sie schnell ein Failover Ihrer gesamten Anwendung in eine Failover-Region durchführen können. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Unterstützte AWS Resilience Hub Ressourcen” • the section called “Identitäts- und Zugriffsverwaltung”	16. November 2022

Aktualisierter Inhalt: Neue Ressourcen für Anwendung skomponenten hinzugefügt	Route53 und AWS Backup wurden der Liste der unterstützten Anwendung skomponenten-Ressourcen im AppComponent Gruppieru ngsbereich hinzugefügt.	01. Juli 2022
Neuer Inhalt: Konzept zum Status der Anwendung skonformität	Der Statustyp „Änderungen erkannt“ wurde hinzugefügt.	2. Juni 2022
Wir stellen vor AWS Resilienc e Hub	AWS Resilience Hub ist jetzt verfügbar. In diesem Leitfaden wird beschrieben, wie Sie AWS Resilience Hub Ihre Infrastruktur analysieren, Empfehlungen zur Verbesser ung der Ausfallsicherheit Ihrer AWS Apps abrufen, Resilienz werte überprüfen und vieles mehr.	10. November 2021

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.