



Benutzerhandbuch

AWS Zentrum für Resilienz



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?	1
AWS Resilience Hub — Resilienzmanagement	2
Wie AWS Resilience Hub funktioniert	2
AWS Resilience Hub — Resilienztests	5
AWS Resilience Hub Konzepte	6
Ausfallsicherheit	6
Recovery Point Objective (RPO)	6
Ziel der Wiederherstellungszeit (RTO)	6
Voraussichtliches Ziel für die Wiederherstellung des Workloads	6
Voraussichtlicher Zielwert für die Wiederherstellung der Arbeitslast	7
Anwendung	7
Komponente der Anwendung	7
Status der Konformität der Anwendung	7
Drift bei der Resilienz	8
Bewertung der Resilienz	8
Bewertung der Resilienz	8
Art der Störung	9
Experimente zur Fehlerinjektion	9
STOPP	10
Unterstützte AWS Resilience Hub Ressourcen	10
Erste Schritte	14
Voraussetzungen	14
Hinzufügen einer Anwendung	15
Schritt 1: Fügen Sie zunächst eine Anwendung hinzu	16
Schritt 2: Verwalten Sie Ihre Anwendungsressourcen	16
Schritt 3: Fügen Sie Ihrer AWS Resilience Hub Anwendung Ressourcen hinzu	17
Schritt 4: Stellen Sie RTO und RPO ein	23
Schritt 5: Richten Sie die Erkennung von Stabilitätsabweichungen ein	24
Schritt 6: Berechtigungen einrichten	25
Schritt 7: Konfigurieren Sie die Konfigurationsparameter der Anwendung	27
Schritt 8: Fügen Sie Ihrer Anwendung Tags hinzu	27
Schritt 9: Überprüfen und veröffentlichen	28
Schritt 10: Führen Sie eine Bewertung durch	28
Verwenden von AWS Resilience Hub	30

Anwendungen	30
Zusammenfassung der Anwendung anzeigen	33
Anwendungsressourcen bearbeiten	36
Gruppieren von Ressourcen in einem AppComponent	44
Veröffentlichen Sie eine neue Anwendungsversion	48
Anwendungsversionen anzeigen	49
Ressourcen Ihrer Anwendung anzeigen	50
Löschen einer Anwendung	52
Konfigurationsparameter der Anwendung	52
Verwaltung von Resilienzrichtlinien	53
Resilienzrichtlinien erstellen	55
Zugreifen auf Details zur Resilienzrichtlinie	58
Resilienzbewertungen	60
Durchführung von Resilienzbewertungen	60
Überprüfung der Bewertungsberichte	61
Resilienzbewertungen werden gelöscht	70
Verwalten von Alarmen	71
Erstellung von Alarmen anhand der Betriebsempfehlungen	71
Alarme anzeigen	74
Standardarbeitsanweisungen	78
Erstellung einer SOP auf der Grundlage von AWS Resilience Hub Empfehlungen	80
Ein benutzerdefiniertes SSM-Dokument erstellen	81
Verwenden Sie ein benutzerdefiniertes SSM-Dokument anstelle des Standarddokuments	82
SOPs testen	82
Standardarbeitsanweisungen anzeigen	82
Experimente mit dem Amazon Fault Injection Service	84
Erstellung von AWS FIS Experimenten auf der Grundlage der Betriebsempfehlungen	85
Durchführung eines AWS FIS Experiments von AWS Resilience Hub	87
Experimente mit Fehlerinjektion anzeigen	88
Fehler beim Amazon Fault Injection Service-Experiment/Statusüberprüfung	91
Grundlegendes zu Resilienzwerten	94
Zugriff auf den Resilienzwert Ihrer Anwendungen	94
Berechnen von Resilienzwerten	97
Integration von Empfehlungen in Anwendungen	113
Änderung der AWS CloudFormation Vorlage	115

Verwendung von AWS Resilience Hub APIs zur Beschreibung und Verwaltung von Anwendungen	120
Vorbereitung des Antrags	120
Erstellen einer Anwendung	120
Erstellen Sie eine Resilienzrichtlinie	121
Importieren Sie die Anwendungsressource und überwachen Sie den Importstatus	122
Veröffentlichen Sie Ihre Anwendung und weisen Sie ihnen eine Ausfallsicherheitsrichtlinie zu	125
Ausführung und Analyse der Anwendung	126
Führen Sie eine Resilienzbewertung durch und überwachen Sie sie	127
Erstellen Sie eine Resilienzrichtlinie	130
Ändern Sie Ihre Bewerbung	145
Manuelles Hinzufügen von Ressourcen	145
Gruppierung von Ressourcen in einer einzigen Anwendungskomponente	146
Ausschließen einer Ressource aus einem AppComponent	148
Sicherheit	150
Datenschutz	150
Verschlüsselung im Ruhezustand	151
Verschlüsselung während der Übertragung	152
Identitäts- und Zugriffsverwaltung	152
Zielgruppe	153
Authentifizierung mit Identitäten	153
Verwalten des Zugriffs mit Richtlinien	158
So funktioniert AWS Resilience Hub mit IAM	160
Richten Sie IAM-Rollen und -Berechtigungen ein	175
Fehlerbehebung	176
AWS Resilience Hub Referenz zu Zugriffsberechtigungen	178
AWS verwaltete Richtlinien	192
Die Terraform-Statusdatei wird importiert in AWS Resilience Hub	201
AWS Resilience Hub Zugriff auf Ihren Amazon EKS-Cluster aktivieren	205
Aktivierung AWS Resilience Hub der Veröffentlichung in Ihren Amazon SNS SNS-Themen	217
Einschränkung der Berechtigungen zum Ein- oder Ausschließen von AWS Resilience Hub Empfehlungen	219
Sicherheit der Infrastruktur	219
Arbeiten mit anderen -Services	221

AWS CloudFormation	221
AWS Resilience Hub- und AWS CloudFormation-Vorlagen	221
Weitere Informationen zu AWS CloudFormation	222
AWS CloudTrail	222
AWS Systems Manager	222
AWS Trusted Advisor	223
Dokumentverlauf	227
AWS-Glossar	254
.....	cclv

Was ist AWS Resilience Hub?

AWS Resilience Hub ist ein zentraler Ort, an dem Sie die Ausfallsicherheit Ihrer Anwendungen verwalten und verbessern können. 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 53 ARC)	Was ist Amazon Route 53 Application Recovery Controller

Themen

- [AWS Resilience Hub — Resilienzmanagement](#)
- [AWS Resilience Hub — Resilienztests](#)
- [AWS Resilience Hub Konzepte](#)
- [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 CI/CD, 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. Zu diesen Richtlinien gehören RTO- und RPO-Ziele für Anwendungen, Infrastruktur, Availability Zone und regionale Störungen. Diese Ziele werden verwendet, um abzuschätzen, ob die Anwendung die Ausfallsicherheitsrichtlinie 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 SOPs für die Wiederherstellung. 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 Ihr geschätzter Workload-RTO und Ihr geschätzter Workload-RPO Ihren RTO- und RPO-Zielen entsprechen.

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, Amazon RDS-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.

Recovery Point Objective (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 Workload-RTO) ist das RTO, das Ihre Anwendung auf der Grundlage der importierten Anwendungsdefinition voraussichtlich einhalten wird. Führen Sie anschließend eine Bewertung durch.

Voraussichtlicher Zielwert für die Wiederherstellung der Arbeitslast

Das geschätzte Ziel für den Workload Recovery Point (geschätztes Workload-RPO) ist das RPO, das Ihre Anwendung auf der Grundlage der importierten Anwendungsdefinition voraussichtlich erfüllen wird. Führen Sie anschließend eine Bewertung durch.

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 zuAWS::ResilienceHub::ComputeAppComponent.

Status der Konformität der Anwendung

AWS Resilience Hub meldet die folgenden Konformitätsstatustypen für Ihre Anwendungen.

Richtlinie erfüllt

Es wird davon ausgegangen, dass die Anwendung die in der Richtlinie festgelegten RTO- und RPO-Ziele erfüllt. Alle Komponenten erfüllen die definierten politischen Ziele. Sie haben beispielsweise ein RTO- und 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 einer Backup-Standardbetriebsprozedur (SOP) durchführen und diese auch testen und zeitlich festlegen. Dies ist in den Betriebsempfehlungen enthalten und Teil Ihres allgemeinen Resilienz-Scores.

Die Richtlinie wurde verletzt

Es konnte nicht davon ausgegangen werden, dass die Anwendung die in der Richtlinie definierten RTO- und RPO-Ziele erfüllt. Eines oder mehrere davon erfüllen die politischen Ziele

nicht. AppComponents Sie haben beispielsweise ein RTO- und RPO-Ziel von 24 Stunden für Störungen 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.

Drift bei der Resilienz

AWS Resilience Hub führt eine Drift-Erkennung durch und führt gleichzeitig eine Bewertung für Ihre Anwendung durch, um zu überprüfen, ob sie mit der Resilienz-Richtlinie konform ist. AWS Resilience Hub verwendet zum Vergleich die Resilienzrichtlinie, die bei der vorherigen erfolgreichen Bewertung der Anwendung definiert wurde.

- Drifted — Weist darauf hin, dass die Anwendung ihre Resilienz-Richtlinie verletzt hat und ein Risiko besteht.
- Nicht verändert — Weist darauf hin, dass sich die Konformität der Anwendung gegenüber der vorherigen Bewertung nicht geändert hat.

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 Standard Operating Procedures (SOPs) ordnungsgemäß funktionieren, um die Anwendung nach dem Ausfall wiederherzustellen.

Tests für SOPs messen den geschätzten Workload-RTO und den geschätzten Workload-RPO. Sie können verschiedene Anwendungskonfigurationen testen und messen, ob das ausgegebene RTO und RPO die in Ihrer Richtlinie definierten Ziele erfüllen.

STOPP

Bei einer Standardarbeitsanweisung (SOP) handelt es sich um eine Reihe vorgeschriebener Schritte, mit denen Sie Ihre Anwendung im Falle eines Ausfalls oder Alarms effizient wiederherstellen können. Auf der Grundlage der Anwendungsbeurteilung werden eine Reihe von SOPs AWS Resilience Hub empfohlen. Es wird empfohlen, SOPs im Vorfeld einer Unterbrechung vorzubereiten, zu testen und zu bewerten, um eine zeitnahe Wiederherstellung sicherzustellen.

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 unter [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

AWS Resilience Hub unterstützt Ressourcen aus den folgenden AWS Diensten:

- Datenverarbeitung
 - Amazon Elastic Compute Cloud (Amazon EC2)
 - AWS Lambda
 - Amazon Elastic Kubernetes Service (Amazon EKS)
 - Amazon Elastic Container Service (Amazon ECS)
 - AWS Step Functions
- Datenbank
 - Amazon Relational Database Service (Amazon RDS)
 - Amazon-DynamoDB
 - Amazon DocumentDB
- Netzwerk und Bereitstellung von Inhalten
 - Amazon Route 53

- Elastic Load Balancing
- Netzwerkadressübersetzung (NAT)
- Speicher
 - Amazon Elastic Block Store (Amazon EBS)
 - Amazon Elastic File System (Amazon EFS)
 - Amazon-Simple-Storage-Service (Amazon-S3)
 - Amazon FSx für Windows File Server
- Weitere
 - Amazon API Gateway
 - Amazon Route 53-Controller für die Anwendungswiederherstellung (Amazon Route 53 ARC)
 - 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 unter [AWS Resilience HubAnwendungsressourcen bearbeiten](#).
- AWS Resilience Hub unterstützt Amazon EKS und Amazon ECS auf AWS Fargate.
- AWS Resilience Hub unterstützt die Bewertung von AWS Backup Ressourcen im Rahmen der folgenden Services:
 - Amazon EBS
 - Amazon EFS
 - Amazon S3
 - Globale Amazon Aurora Aurora-Datenbank

- Amazon-DynamoDB
- Amazon RDS-Dienste
- Amazon FSx für Windows File Server
- Amazon Route 53 ARC in AWS Resilience Hub bewertet nur Amazon DynamoDB Global, Elastic Load Balancing, Amazon RDS 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 einem AppComponent](#)
- Unterstützt derzeit AWS Resilience Hub keine regionsübergreifenden Bewertungen für Amazon EKS-Cluster, wenn sich entweder der Amazon EKS-Cluster befindet oder wenn die Anwendung in einer Region erstellt wurde, für die das 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 den geschätzten Arbeitslast-RTO oder den geschätzten Workload-RPO auswirken — Ressourcen wie `AWS::RDS::DBParameterGroup`, die sich nicht auf den geschätzten Workload-RTO oder den geschätzten Workload-RPO auswirken, werden von ignoriert. AWS Resilience Hub
- 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-GW HTTP) 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 Amazon RDS-Instance gruppiert werden. Weitere Informationen zur Bearbeitung von Ressourcen finden Sie unter [the 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.

Voraussetzungen

Bevor Sie den 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 unter [the section called “So funktioniert AWS Resilience Hub mit IAM”](#). Weitere Informationen zum Hinzufügen einer Richtlinie zur Rolle finden Sie unter [the section called “Definition der Vertrauensrichtlinie mithilfe der 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 über von AWS verwaltete Richtlinien finden Sie unter [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

Eine Anwendung hinzufügen 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 Recovery Time Objective (RTO) und Recovery Point Objective (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 der geschätzte Workload-RTO und der geschätzte Workload-RPO Ihre RTO- und RPO-Ziele erreichen.

Themen

- [Schritt 1: Fügen Sie zunächst eine Anwendung hinzu](#)
- [Schritt 2: Wie wird Ihre Anwendung verwaltet?](#)
- [Schritt 3: Fügen Sie Ihrer AWS Resilience Hub Anwendung Ressourcen hinzu](#)
- [Schritt 4: Stellen Sie RTO und RPO ein](#)

- [Schritt 5: Drift-Erkennung](#)
- [Schritt 6: Berechtigungen einrichten](#)
- [Schritt 7: Konfigurieren Sie die Konfigurationsparameter der Anwendung](#)
- [Schritt 8: Schlagworte hinzufügen](#)
- [Schritt 9: Überprüfe und veröffentliche deine AWS Resilience Hub Bewerbung](#)
- [Schritt 10: Führen Sie eine Bewertung Ihrer AWS Resilience Hub Bewerbung durch](#)

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 EKS) -Clustern befinden. Das heißt, mit AWS Resilience Hub können

Sie Ressourcen, die sich auf Ihren Amazon EKS-Clustern befinden, als optionale Ressourcen hinzufügen. 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”](#)

- **Nur EKS** — Wählen Sie diese Option, wenn Sie Ressourcen aus Namespaces innerhalb der Amazon EKS-Cluster ermitteln möchten.

Wenn Sie diese Option auswählen, müssen Sie das Verfahren in abschließen [the section called “Fügen Sie EKS-Cluster hinzu”](#)

- **Ressourcensammlungen und EKS** — Wählen Sie diese Option, wenn Sie Ressourcen aus einer der Ressourcensammlungen und Amazon EKS-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 [the section called “Fügen Sie EKS-Cluster hinzu”](#).

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 EKS-Cluster hinzu”](#)

Fügen Sie Ressourcensammlungen hinzu

In diesem Abschnitt werden die folgenden Methoden beschrieben, die Sie verwenden, um die Grundlage für Ihre Anwendungsstruktur zu 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 stammenden 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 Stack außerhalb der AWS Region hinzufügen ein und wählen Sie dann Stack-ARN hinzufügen. Weitere Informationen zur Verwendung von ARNs finden Sie unter [Amazon-Ressourcennamen \(ARNs\)](#) in der Allgemeinen AWS -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 Feld Ressourcengruppen-ARN ein und wählen Sie dann Ressourcengruppen-ARN hinzufügen. Weitere Informationen zur Verwendung von ARNs finden Sie unter [Amazon-Ressourcennamen \(ARNs\)](#) in der Allgemeinen AWS -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 in das Feld S3-URL ein und wählen Sie S3-URL hinzufügen aus.

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 EKS-Cluster hinzu

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

Note

Sie benötigen Amazon EKS-Berechtigungen und zusätzliche IAM-Rollen, um eine Verbindung zum Amazon EKS-Cluster herzustellen. Weitere Informationen zum Hinzufügen von Amazon EKS-Berechtigungen für einzelne Konten und kontoübergreifende Amazon EKS-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 Amazon EKS-Cluster aktivieren”](#)

Wählen Sie die Amazon EKS-Cluster und -Namespaces aus, die die Ressourcen enthalten, die Sie in der von Ihnen beschriebenen Anwendung verwenden möchten. Die Amazon EKS-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 Amazon EKS-Cluster zu bewerten, müssen Sie die entsprechenden Namespaces manuell zu jedem der Amazon EKS-Cluster im Abschnitt EKS-Cluster und Namespaces hinzufügen. Der Namespace-Name muss exakt mit dem Namespace-Namen auf Ihren Amazon EKS-Clustern übereinstimmen.

So fügen Sie Amazon EKS-Cluster hinzu

1. Wählen Sie die Amazon EKS-Cluster aus der Dropdownliste EKS-Cluster auswählen aus, die Ihrer Region AWS-Konto und Ihrer Region zugeordnet sind.
2. Um Amazon EKS-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 EKS-ARN hinzufügen. Weitere Informationen zur Verwendung von ARNs finden Sie unter [Amazon-Ressourcennamen \(ARNs\)](#) in der Allgemeinen AWS -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 Amazon EKS-Cluster aktivieren”](#)

So fügen Sie Namespaces aus den ausgewählten Amazon EKS-Clustern hinzu

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

Sie können Amazon EKS-Cluster wie folgt identifizieren:

- EKS-Clustername — Gibt den Namen der ausgewählten Amazon EKS-Cluster an.
 - Anzahl der Namespaces — Gibt die Anzahl der Namespaces an, die in den Amazon EKS-Clustern ausgewählt wurden.
 - Status — Gibt an, ob AWS Resilience Hub die Namespaces der ausgewählten Amazon EKS-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 EKS-Cluster aufgenommen haben.
 - Namespaces hinzugefügt — Zeigt an, dass Sie einen oder mehrere Namespaces aus dem Amazon EKS-Cluster hinzugefügt haben.
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 Amazon EKS-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 Amazon EKS-Cluster übereinstimmen.
- Um einen Namespace zu entfernen, wählen Sie Entfernen neben dem Namespace aus.
 - Um die ausgewählten Namespaces auf alle Amazon EKS-Cluster anzuwenden, wählen Sie Namespaces auf alle EKS-Cluster anwenden.

Wenn Sie diese Option wählen, wird Ihre vorherige Namespace-Auswahl in den anderen Amazon EKS-Clustern durch die aktuelle Namespace-Auswahl überschrieben.

4. Um die aktualisierten Namespaces in Ihre Anwendung aufzunehmen, wählen Sie Aktualisieren.

Next

[Schritt 4: Stellen Sie RTO und RPO ein](#)

Schritt 4: Stellen Sie RTO und RPO ein

Sie können eine neue Ausfallsicherheitsrichtlinie mit Ihren eigenen RTO/RPO-Zielen definieren oder Sie können eine bestehende Ausfallsicherheitsrichtlinie mit vordefinierten RTO/RPO-Zielen auswählen. Wenn Sie eine der vorhandenen Resilienzrichtlinien verwenden möchten, wählen Sie Bestehende Richtlinienoption 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 Ihr RTO/RPO im Abschnitt RTO/RPO-Ziele.

Note

- Wir haben ein Standard-RTO und -RPO für Ihre Anwendung eingegeben. Sie können RTO und RPO jetzt oder nach der Prüfung der Anwendung ändern.
- AWS Resilience Hub ermöglicht es Ihnen, den Wert Null in die Felder RTO und RPO Ihrer Ausfallsicherheitsrichtlinie einzugeben. Bei der Bewertung Ihrer Anwendung liegt das niedrigstmögliche Bewertungsergebnis jedoch nahe Null. Wenn Sie also in die Felder RTO und RPO einen Wert von Null eingeben, liegen die Ergebnisse für den geschätzten Workload RTO und den geschätzten Workload-RPO nahe Null, und der Compliance-Status für Ihre Anwendung wird auf Policy Breached gesetzt.

5. Um RTO/RPO für Ihre Infrastruktur und AZ zu definieren, klicken Sie auf den Rechtspfeil, um den Abschnitt Infrastruktur-RTO und RPO zu erweitern.
6. Geben Sie unter RTO/RPO-Ziele einen numerischen Wert in das Feld ein und wählen Sie dann die Zeiteinheit aus, für die der Wert sowohl für RTO als auch für RPO steht.

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

7. (Optional) Wenn Sie über eine Anwendung mit mehreren Regionen verfügen und RTO und RPO für Regionen definieren möchten, aktivieren Sie Region — Optional.

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

Next

[the section called “Schritt 5: Richten Sie die Erkennung von Stabilitätsabweichungen ein”](#)

Schritt 5: Drift-Erkennung

Mit AWS Resilience Hub können Sie die Erkennung von Resilienzabweichungen einrichten, um Ihre Anwendung täglich zu bewerten und benachrichtigt zu werden, wenn Abweichungen festgestellt werden oder wenn eine Bewertung fehlgeschlagen ist.

So richten Sie die Erkennung von Resilienzabweichungen ein

1. Um Ihre Anwendung täglich zu bewerten, aktivieren Sie die Option Diese Anwendung 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 `AwsResilienceHubPeriodicAssessmentRole`

Rolle mithilfe des entsprechenden Verfahrens in [the section called “So funktioniert AWS Resilience Hub mit IAM”](#).

2. Um benachrichtigt zu werden, wenn AWS Resilience Hub Abweichungen im Konformitätsstatus festgestellt werden oder wenn die tägliche Resilienzbewertung fehlschlägt, aktivieren Sie die Option Bei Verstößen gegen die Resilienz-Richtlinien benachrichtigen lassen.

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

 Note

- Damit AWS Resilience Hub Benachrichtigungen zu Ihren Amazon SNS SNS-Themen veröffentlichen kann, muss Ihr Amazon SNS SNS-Thema mit den entsprechenden Berechtigungen konfiguriert sein. Weitere Informationen zur Konfiguration von Berechtigungen finden Sie unter [the section called “Aktivierung AWS Resilience Hub der Veröffentlichung in Ihren Amazon SNS SNS-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 Amazon SNS SNS-Themen zu verwenden, die sich in einer anderen AWS-Konto oder einer anderen Region oder in beiden befinden, wählen Sie SNS-Thema eingeben und geben Sie den Amazon-Ressourcennamen (ARN) des Amazon SNS-Themas in das Feld SNS-Thema angeben ein. Weitere Informationen zur Verwendung von ARNs finden Sie unter [Amazon-Ressourcennamen \(ARNs\)](#) in der Allgemeinen AWS -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 Wählen Sie eine IAM-Rolle aus.

Note

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

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

- AWS IAM-Konsole — Wenn Sie diese Option wählen, müssen Sie das Verfahren unter So erstellen Sie Ihre AWS Resilience Hub-Rolle in der IAM-Konsole abschließen.
 - AWS CLI — Wenn Sie diese Option wählen, müssen Sie alle Schritte in AWS CLI ausführen.
 - CloudFormation Vorlage — Wenn Sie diese Option wählen, müssen Sie je nach Kontotyp (primäres Konto oder sekundäres Konto) die Rollen mithilfe der entsprechenden AWS CloudFormation Vorlage erstellen.
2. Klicken Sie auf den Rechtspfeil, um den Abschnitt IAM-Rolle (n) aus einem kontoübergreifenden Konto hinzufügen — Optional zu erweitern.
 3. Um IAM-Rollen aus einem Cross-Account auszuwählen, geben Sie die ARNs der IAM-Rolle in das Feld Eine IAM-Rolle ARN ein. Stellen Sie sicher, dass die ARNs der IAM-Rollen, die Sie eingeben, nicht zum aktuellen Konto gehören.
 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 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 Erkennung von Resilienzabweichungen) möglicherweise nicht wie erwartet und die Eingaben, die Sie in Schritt 1 und Schritt 3 eingegeben haben, werden ignoriert.

Next

[Schritt 8: Schlagworte hinzufügen](#)

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 unter [Konfigurationsparameter 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: Schlagworte hinzufügen](#)

Schritt 8: Schlagworte hinzufügen

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 von AWS Resilience Hub

AWS Resilience Hub hilft Ihnen, die Resilienz Ihrer Anwendungen zu verbessern und AWS und reduzieren Sie die Wiederherstellungszeit bei Anwendungsausfällen.

Zu verwenden AWS Resilience Hub, du:

- Beschreibe dein AWS Bewerbungen in AWS Resilience Hub.
- Verwalte deine AWS Ressourcen in AWS Resilience Hub.
- Erstellen Sie effektive Resilienzrichtlinien.
- Führen Sie Bewertungen durch, die auf die Resilienz Ihrer Anwendungen hinweisen.
- Verwalten Sie Alarme, Standardarbeitsanweisungen (SOPs) und Tests für Ihre Anwendungen.

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 Ihr geschätzter Workload-RTO und Ihr geschätzter Workload-RPO Ihren RTO- und RPO-Zielen entsprechen.

AWS Resilience Hub zeigt die Vorgängerversionen Ihrer Anwendung ab dem Zeitpunkt ihrer Erstellung an, damit Sie Änderungen an der Anwendung leichter nachverfolgen können. AWS Resilience Hub Diese Transparenz hilft Ihnen, frühere Anwendungskonfigurationen zu überprüfen und Entscheidungen über die aktuelle Anwendungskonfiguration zu treffen. AWS Resilience Hub verwendet die folgenden Status, um die Anwendungsversionen zu identifizieren:

- Entwurf — Zeigt an, dass die Anwendungsversion geändert wird und noch veröffentlicht werden muss.
- Aktuelle Version — Zeigt an, dass es sich bei dieser Anwendungsversion um die zuletzt veröffentlichte Version handelt. AWS Resilience Hub verwendet diese Anwendungsversion für die Durchführung von Resilienzbewertungen.
- Alle Versionen anzeigen — Wählen Sie das Pluszeichen (+), um alle vorherigen Versionen schreibgeschützt anzuzeigen.

Sie können Ihre Anwendungen auf der Anwendungsseite 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 (RPO) nicht erfüllt hat. Lesen Sie die Empfehlungen von und verwenden Sie sie, AWS Resilience Hub bevor Sie Ihre Anwendung erneut im Hinblick auf die Ausfallsicherheit bewerten. Weitere Informationen zu Empfehlungen finden Sie unter [Eine Anwendung hinzufügen 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 unter [Ausfallsicherheit 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.
- **Ausfallstatus** — Zeigt an, ob Ihre Anwendung von der vorherigen erfolgreichen Bewertung 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.
 - **Nicht verändert** — Zeigt an, dass die Anwendung weiterhin voraussichtlich die in der Richtlinie definierten RTO- und RPO-Ziele erreicht.
- **Geschätzter Workload-RTO** — Gibt den maximal möglichen geschätzten Workload-RTO Ihrer Anwendung an. Dieser Wert ist der maximale geschätzte Workload-RTO aller Störungstypen aus der letzten erfolgreichen Bewertung.
- **Geschätztes Workload-RPO** — Gibt das maximal mögliche geschätzte Workload-RPO Ihrer Anwendung an. Dieser Wert ist der maximale geschätzte Workload-RTO aller Störungstypen aus der letzten erfolgreichen Bewertung.
- **Uhrzeit der letzten Bewertung** — 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 zur Verwendung von ARNs finden Sie unter [Amazon-Ressourcennamen \(ARNs\)](#) in der Allgemeinen AWS-Referenz.

Note

AWS Resilience Hub kann die Resilienz regionsübergreifender Amazon ECS-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](#)
- [AWS Resilience HubAnwendungsressourcen bearbeiten](#)
- [Gruppieren von Ressourcen in einem AppComponent](#)
- [Veröffentlichung einer neuen AWS Resilience Hub Anwendungsversion](#)
- [Alle Versionen der AWS Resilience Hub Anwendung anzeigen](#)
- [Ressourcen der AWS Resilience Hub Anwendung anzeigen](#)
- [Eine AWS Resilience Hub Anwendung löschen](#)
- [Konfigurationsparameter der Anwendung](#)

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 Applications (Anwendungen).
2. Wählen Sie auf der Seite „Anwendungen“ den Namen der Anwendung aus.

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

Themen

- [Details](#)
- [Ausfallsicherheit von Anwendungen](#)
- [Alarmer wurden implementiert](#)
- [Experimente wurden durchgeführt](#)

Details

Der Abschnitt „Details zur Anwendungsübersicht“ enthält eine Zusammenfassung der Auswahlmöglichkeiten für die Anwendung.

- **Bewerbungsstatus** — Gibt an, ob Ihre Bewerbung aktiv ist oder nicht.
- **Beschreibung** — Die Beschreibung Ihrer Bewerbung.
- **Konformitätsstatus** — Zeigt den Konformitätsstatus Ihrer Anwendung an.
- **Zuletzt geprüft am** — Gibt das Datum und die Uhrzeit an, zu der Ihr Antrag zuletzt geprüft wurde.
- **Ausfallsicherheitsrichtlinie** — Zeigt den Namen der Resilienzrichtlinie an, die Ihrer Anwendung zugeordnet ist. Weitere Informationen zu Resilienzrichtlinien finden Sie unter [Verwaltung von Resilienzrichtlinien](#)
- **Geplante Bewertung** — Gibt an, ob die tägliche Bewertung aktiv oder inaktiv ist.
- **Status der Resilienz** — Gibt an, ob Ihre Anwendung von der vorherigen erfolgreichen Bewertung abweicht oder nicht.
- **Letzte Abweichung am** — Gibt das Datum und die Uhrzeit an, zu der Ihre Bewerbung auf Abweichungen geprüft wurde.

Um die geplante Bewertung zu aktualisieren

1. Um die geplante Bewertung für Ihre Anwendung zu aktualisieren, wählen Sie unter Aktionen die Option Resiliency Drift Detection aktualisieren aus.
2. Um die Erkennung von Resilienzabweichungen zu aktualisieren, führen Sie die Schritte unter [Schritt 5: Drift-Erkennung](#), und kehren Sie dann zu diesem Verfahren zurück.
3. Wählen Sie Aktualisieren aus.

Note

Um die Erkennung von Resilienzabweichungen für bestehende Anwendungen zu aktivieren, müssen Sie manuell eine Bewertung durchführen, nachdem Sie die Funktion zur Erkennung von Resilienzabweichungen zum ersten Mal aktiviert haben. Weitere Informationen zur Durchführung von Bewertungen finden Sie unter [Durchführung von Resilienzbewertungen](#)

Ausfallsicherheit von Anwendungen

Die im Abschnitt Ausfallsicherheit von Anwendungen angezeigten Kennzahlen stammen aus der letzten Resilienzbewertung der Anwendung.

Bewertung der Resilienz

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 die richtige SOP auslöst.

Nehmen wir zum Beispiel an, dass ein Test mit einem Alarm und einer SOP AWS Resilience Hub empfohlen wird. Wenn der Test ausgeführt wird, initiiert der Alarm die zugehörige SOP und wird dann erfolgreich ausgeführt. Weitere Informationen zur Resilienzbewertung finden Sie unter [Grundlegendes zu Resilienzwerten](#)

Resilienzbewertung im Zeitverlauf

Anhand des Resilienz-Scores im Zeitverlauf können Sie sich ein Diagramm der Resilienz 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 zu geplanten Assessments finden Sie unter [Schritt 5: Drift-Erkennung](#).

Note

AWS Resilience Hub führt geplante Prüfungen 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 anzuzeigen in CloudWatch, um detailliertere Informationen zur Ausfallsicherheit Ihrer Anwendung in Ihrem CloudWatch Dashboard zu erstellen und anzuzeigen. Weitere Informationen dazu finden Sie CloudWatch unter [Verwenden von Dashboards](#) im CloudWatch Amazon-Benutzerhandbuch.

Alarmer wurden implementiert

In der Anwendungsübersicht „Implementierte Alarmer“ werden die Alarmer aufgeführt, die Sie in Amazon CloudWatch zur Überwachung der Anwendung eingerichtet haben. Weitere Informationen zu Alarmen finden Sie unter [Verwalten 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 unter [Experimente mit dem Amazon Fault Injection Service](#).

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 Resilienz 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 Run (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 „Überprüfen“ für den Bewertungsbericht Ihrer Anwendung.

Um die Erkennung von Stabilitätsabweichungen 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 Erkennung von Resilienzabweichungen aktivieren oder deaktivieren möchten.

3. Wählen Sie unter Aktionen die Option Erkennung von Resilienzabweichungen aktualisieren aus.
4. Um die Erkennung von Resilienzabweichungen zu aktualisieren, führen Sie die Schritte unter [aus Schritt 5: Drift-Erkennung](#), und kehren Sie dann zu diesem Verfahren zurück.
5. Wählen Sie Aktualisieren aus.

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 [aus Schritt 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 Attach (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.
 - **Quellentyp** — 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 die Option Eingabequellen hinzufügen aus. Weitere Informationen zum Hinzufügen von Eingabequellen finden Sie unter [the 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 unter [the 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 einem AppComponent](#)
- **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.
- **Quellentyp** — 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** — Dies 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.
- **AppComponent** — 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 wählen Sie dann unter Aktionen die Option Stacks aktualisieren aus.
 - b. Um Ihre Ressourcen zu aktualisieren, führen Sie auf der Seite Stacks aktualisieren die entsprechenden Verfahren unter [aus Schritt 3: Fügen Sie Ihrer AWS Resilience Hub Anwendung Ressourcen hinzu](#), und kehren Sie dann zu diesem Verfahren zurück.
 - c. Wählen Sie Speichern aus.
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 Add (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 aus.
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 aus.

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 Add (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 unter [Gruppieren von Ressourcen in einem AppComponent](#).

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 weitergeleitetAWS 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 aus.
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 unter [Veröffentlichung einer neuen AWS Resilience Hub Anwendungsversion](#).

Gruppieren von Ressourcen in einem AppComponent

Eine 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 Anwendungskomponente (AppComponent). AWS Resilience Hub enthält Regeln, die festlegen, welche AWS Ressourcen zu welchem Typ gehören können. AppComponent Zum Beispiel DBInstance kann a gehören, `AWS::ResilienceHub::DatabaseAppComponent` aber nicht zu `AWS::ResilienceHub::ComputeAppComponent`.

Wenn die Anwendung AWS Resilience Hub mit einem AWS CloudFormation Stack, einer Terraform-Statusdatei AWS Resource Groups, einem Amazon Elastic Kubernetes Service Service-Cluster oder einer AppRegistry Anwendung importiert wird, bemüht man sich nach besten Kräften, AWS Resilience Hub verwandte Ressourcen zu denselben zu gruppieren AppComponent, ist aber möglicherweise nicht immer hundertprozentig genau. Sie kennen die Architektur Ihrer Anwendung am besten, sodass Sie Ressourcen, die bereits nach Gruppen gruppiert wurden, in andere zusammenfassen können. AWS Resilience Hub AppComponent Wenn Sie beispielsweise drei EC2-Instances in einem AWS CloudFormation Stack haben, AWS Resilience Hub wird eine einzelne AppComponent pro EC2-Instance erstellt, aber auf allen drei EC2-Instances wird möglicherweise

dieselbe Anwendungssoftware ausgeführt. In diesem Fall besteht die richtige Wahl darin, die drei EC2-Instances zu einer einzigen zusammenzufassen. ComputeAppComponent Wenn Sie Ressourcen neu gruppieren, sollten Sie die Ressource nur zu einer Ressource umgruppieren. AppComponent Sie können Ihre Ressourcenliste auch erweitern und nicht gruppierte Ressourcen zu einer zusammenfassen. AppComponent

Sie AWS Resilience Hub AppComponent 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`

Im Folgenden finden Sie Beispiele für korrekte Gruppierungen:

- Gruppieren Sie Primärdatenbanken und Replikat in einer einzigen Datenbank. AppComponent
- Gruppieren Sie einen Amazon S3 S3-Bucket und seine Replikation unter einem einzigen AppComponent.
- Gruppieren Sie Amazon EC2 EC2-Instances, die dieselbe Anwendung ausführen, unter einer einzigen AppComponent.
- Gruppieren Sie eine Amazon SQS SQS-Warteschlange und ihre Warteschlange für unzustellbare Briefe zu einer einzigen. AppComponent
- Gruppieren Sie Amazon ECS-Services in einer Region und führen Sie Failover von Amazon ECS-Services in einer anderen Region unter einer einzigen AppComponent Region durch.

 Note

AWS Resilience Hub erfordert die richtige Gruppierung, damit das geschätzte Workload-RTO und das geschätzte Workload-RPO zur Generierung von Empfehlungen berechnet werden können.

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. Wählen Sie die Ressource aus, die Sie neu gruppieren möchten.
7. Wählen Sie unter Aktionen die Option Ändern AppComponent aus.

Das AppComponent Dialogfeld „Ändern“ wird angezeigt.

8. Um den aktuellen Namen AppComponent aus dem AppComponentAbschnitt 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 AppComponent aus dem AppComponentTab.
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.

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. Wählen Sie die Ressourcen aus, die Sie gruppieren möchten.

 Note

Sie können nicht manuell hinzugefügte Ressourcen auswählen.

7. Wählen Sie Aktionen und anschließend Gruppenressourcen aus.

Das AppComponent Fenster Kombinieren wird angezeigt.

8. Wählen Sie AppComponent aus der AppComponent Dropdownliste „Wählen“ eine aus, in der Sie die Ressource gruppieren möchten.
9. Wählen Sie Speichern.
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.

Veröffentlichung einer neuen AWS Resilience Hub Anwendungsversion

Nachdem Sie, wie unter beschrieben, Änderungen an Ihren AWS Resilience Hub Anwendungsressourcen vorgenommen haben [AWS Resilience Hub Anwendungsressourcen bearbeiten](#), müssen Sie eine neue Version Ihrer Anwendung veröffentlichen, um eine genaue Resilienzbewertung durchführen zu können. Möglicherweise müssen Sie auch eine neue Version Ihrer Anwendung veröffentlichen, wenn Sie Ihrer Anwendung neue empfohlene Alarme, SOPs 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 Resilienzberichtsbericht 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 unter [the 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 Amazon EC2 EC2-Instance. Weitere Informationen zum Gruppieren von AppComponent Ressourcen finden Sie unter [Gruppieren von Ressourcen in einem AppComponent](#)
- **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.
- **Quellentyp** — 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 Amazon EKS-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 Amazon EC2 EC2-Instance-ID oder ein S3-Bucket-Name.
 - **Inbegriffen** — Dies gibt an, ob diese Ressourcen in der Anwendung AWS Resilience Hub 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 aus.
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 durch [the 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 AWSallgemeinen 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 AWSallgemeinen 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 Resilienz-Richtlinie 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 Edit (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. 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. SOP-Empfehlungen stellen Skripts zur Verfügung, mit denen gängige Wiederherstellungsprozesse verwaltet werden können, z. B. die Wiederherstellung aus einem Backup. Die Testempfehlungen bieten 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 SOPs unter den von Ihnen angegebenen Bedingungen funktionieren.

Durchführung von Resilienzbewertungen

Sie können einen Bericht zur Resilienzbewertung von mehreren Standorten in ausführen. AWS Resilience Hub Weitere Informationen zu Ihrer Anwendung finden Sie unter [the section called “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 „Assessments“ 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 Widerstandsfähigkeit.
- 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 RTO- und 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.

RTO

Zeigt in grafischer Darstellung, ob die Anwendung voraussichtlich die Ziele der Resilienz-Richtlinie 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 RTO-Workload an.

RPO

Zeigt in grafischer Darstellung, ob die Anwendung voraussichtlich die Ziele der Resilienz-Richtlinie erfüllt. Dies basiert auf der Zeitspanne, in der Daten verloren gehen können, bevor ein erheblicher Schaden für das Unternehmen eintritt. Die Bewertung liefert einen geschätzten RPO-Wert für die Arbeitslast.

Details

Enthält detaillierte Beschreibungen der einzelnen Störungstypen mithilfe der Registerkarten. Alle Ergebnisse und Abweichungen bei der Anwendungskonformität. 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.

- Geschätzter RTO

Gibt an, ob Ihre Richtlinienkonfiguration Ihren Richtlinienanforderungen entspricht. Wir geben zwei Werte an: unseren geschätzten RTO und Ihren angestrebten RTO. Wenn Sie beispielsweise unter Ziel-RTO einen Wert von 2 Stunden und unter RTO für geschätzte Arbeitslast einen Wert von 40 Mio. sehen, bedeutet das, dass wir einen geschätzten Workload-RTO von 40 Minuten angeben, während der aktuelle RTO Ihrer Anwendung zwei Stunden beträgt. Wir stützen unsere geschätzte RTO-Berechnung für die Arbeitslast auf die Konfiguration, nicht auf die Richtlinie. Daher hat eine Multi-Availability Zone-Datenbank bei einem Ausfall der Availability Zone immer den gleichen geschätzten Workload-RTO, unabhängig davon, welche Richtlinie Sie wählen.

- RTO-Drift

Gibt die Dauer an, um die Ihre Anwendung von der geschätzten Arbeitslast (RTO) der vorherigen erfolgreichen Prüfung abgewichen ist. Wir geben zwei Werte an, unseren geschätzten RTO und den RTO-Drift. Wenn Sie beispielsweise unter „Geschätzte RTO“ einen Wert von 2 Stunden und unter „RTO-Drift“ einen Wert von 40 Minuten sehen, bedeutet dies, dass Ihre Anwendung von der geschätzten Workload-RTO der vorherigen erfolgreichen Bewertung um 40 Minuten abweicht.

- Geschätztes RPO

Zeigt die tatsächliche RPO-Richtlinie „Geschätzte Arbeitslast“ an, die AWS Resilience Hub auf der Grundlage der Ziel-RPO-Richtlinie geschätzt wird, die Sie für jede Anwendungskomponente festgelegt haben. 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- und RPO-Ziel, das Sie nicht angeben können, ist Region. Bei einigen Anwendungen ist es sinnvoll, die Wiederherstellung zu planen, wenn eine entscheidende Abhängigkeit von einem AWS-Service besteht, der möglicherweise in der gesamten Region nicht mehr verfügbar ist.

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

- RPO-Drift

Gibt die Dauer an, um die Ihre Anwendung vom geschätzten Workload-RPO der vorherigen erfolgreichen Prüfung abgewichen ist. Wir geben zwei Werte an: unseren geschätzten RPO und den RPO-Drift. Wenn Sie beispielsweise unter „Geschätztes RPO“ einen Wert von 2 Stunden und unter „RPO-Drift“ 40 m sehen, bedeutet dies, dass Ihre Anwendung vom geschätzten Workload-RPO der vorherigen erfolgreichen Bewertung um 40 Minuten abweicht.

Überprüfung der Empfehlungen zur Ausfallsicherheit

In den Empfehlungen zur Ausfallsicherheit werden die Anwendungskomponenten bewertet und es werden Empfehlungen zur Optimierung anhand des geschätzten Workload-RTO und des geschätzten Workload-RPO, der Kosten und der minimalen Änderungen gegeben.

Mit AWS Resilience Hub können Sie die Ausfallsicherheit mithilfe einer der folgenden empfohlenen Optionen unter Warum sollten Sie sich für diese Option entscheiden, optimieren:

Note

- AWS Resilience Hub bietet bis zu drei AWS Resilience Hub empfohlene Optionen.
- Wenn Sie regionale RTO- und RPO-Ziele festlegen, AWS Resilience Hub wird in den empfohlenen Optionen die Option Für Region RTO/RPO optimieren angezeigt. Wenn keine regionalen RTO- und RPO-Ziele festgelegt sind, wird RTO/RPO für Availability Zone (AZ) optimieren angezeigt. Weitere Informationen zur Festlegung regionaler RTO/RPO-Ziele bei der Erstellung von Ausfallsicherheitsrichtlinien finden Sie unter [Resilienzrichtlinien erstellen](#)
- Die geschätzten RTO-Werte für die Arbeitslast und die geschätzten RPO-Werte für die Arbeitslast für die Anwendungen und ihre Konfigurationen werden unter Berücksichtigung der Datenmenge und der einzelnen Benutzer bestimmt. AppComponents 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.

Optimieren Sie für Availability Zone RTO/RPO

Die niedrigstmöglichen geschätzten Workload-Wiederherstellungszeiten (RTO/RPO) während einer Unterbrechung der Availability Zone (AZ). Wenn Ihre Konfiguration nicht ausreichend geändert werden kann, um die RTO- und RPO-Ziele zu erreichen, werden Sie über die niedrigsten geschätzten

Wiederherstellungszeiten für Workloads in AZ informiert, damit Ihre Konfiguration der Möglichkeit nahe kommt, die Richtlinie einzuhalten.

Optimieren Sie für die Region RTO/RPO

Die niedrigstmögliche geschätzte Workload-Wiederherstellungszeit (RTO/RPO) während einer regionalen Störung. Wenn Ihre Konfiguration nicht ausreichend geändert werden kann, um die RTO- und RPO-Ziele zu erreichen, werden Sie über die niedrigsten geschätzten Wiederherstellungszeiten für die Workload-Region 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, 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 Discount Program (EDP).

- Geschätzte Arbeitslast (RTO und RPO)

Das geschätzte Workload-RTO und das geschätzte Workload-RPO nach Änderungen.

AWS Resilience Hub bewertet, ob eine Anwendungskomponente (AppComponent) eine Ausfallsicherheitsrichtlinie einhalten kann. Wenn der einer Ausfallsicherheitsrichtlinie AppComponent nicht entspricht und AWS Resilience Hub keine Empfehlungen zur Erleichterung der Einhaltung aussprechen kann, kann dies daran liegen, dass die Wiederherstellungszeit für die ausgewählten Geräte 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, SOPs und AWS FIS Experimenten anhand AWS CloudFormation von Vorlagen.

AWS Resilience Hub stellt AWS CloudFormation Vorlagendateien bereit, mit denen Sie die Infrastruktur der Anwendung als Code herunterladen und verwalten können. Daher 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-URI anzugeben, anstatt CLI/API mit lokaler Datei als Eingabe zu verwenden.

In AWS Resilience Hub können Sie die folgenden Aktionen ausführen:

- Sie können die ausgewählten Alarme, SOPs und AWS FIS Experimente bereitstellen. Um Alarme, SOPs und AWS FIS Experimente bereitzustellen, 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 eine Amazon Simple Storage Service (Amazon S3) -URL auf Ihre erstellten Vorlagen zugreifen.
- Sie können ausgewählte Alarme, SOPs und AWS FIS Experimente, 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 sich alle zugehörigen Tags anzeigen lassen.

Einschließlich oder ohne betriebliche Empfehlungen

AWS Resilience Hub bietet eine Option zum Ein- oder Ausschließen der Alarme, SOPs und AWS FIS Experimente (Tests), die zur Verbesserung der Ausfallsicherheit Ihrer Anwendung zu einem beliebigen Zeitpunkt empfohlen wurden. 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, 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 auszuschließen

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

- a. Wählen Sie auf der Registerkarte Standardarbeitsanweisungen in der Tabelle SOPs alle SOPs (mit dem Status Implementiert oder Nicht implementiert) aus, die Sie ausschließen möchten. Den aktuellen Implementierungsstatus einer SOP können Sie der Spalte Status entnehmen.
- b. Wählen Sie unter Aktionen die Option Ausgewählte ausschließen aus, um die ausgewählten SOPs aus Ihrer Anwendung auszuschließen.
- c. Wählen Sie im Dialogfeld „Empfehlungen ausschließen“ einen der folgenden Gründe aus (optional) und wählen Sie Ausgewählte ausschließen aus, um die ausgewählten SOPs aus der Anwendung auszuschließen.
 - Bereits implementiert — Wählen Sie diese Option, wenn Sie diese SOPs bereits in einem AWS Service oder einem anderen Drittanbieter implementiert haben.
 - Nicht relevant — Wählen Sie diese Option, wenn die SOPs nicht Ihren Geschäftsanforderungen entsprechen.
 - Zu kompliziert in der Implementierung — Wählen Sie diese Option, wenn Sie der Meinung sind, dass die Implementierung dieser SOPs zu kompliziert ist.
 - Keine — Wählen Sie diese Option, wenn Sie den Grund nicht angeben möchten.

2. Gehen Sie wie folgt vor, um SOPs einzubeziehen:

- a. Wählen Sie auf der Registerkarte Standardarbeitsanweisungen in der Tabelle SOPs 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 aus, um alle ausgewählten SOPs in Ihre Anwendung aufzunehmen.

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, 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 einzubeziehen.

Resilienzbewertungen werden gelöscht

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 mit 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](#)
- [Alarme anzeigen](#)

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 eine Amazon S3 S3-URL darauf zugreifen, sie herunterladen und in Ihrer Code-Pipeline platzieren 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 Alarmentabelle 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 Alarmentabelle 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 Alarmentabelle 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 für Amazon bereitgestellt wurden CloudWatch, der Status in Amazon jedoch auf INSUFFICIENT_DATA gesetzt ist. CloudWatch Wenn Sie die unten stehende Zahl auswählen, wird die Alarmentabelle 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 aus, die unter demselben liegt.
 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 Erstellen. 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 — Der 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 Link SOP-Ordner aus.
4. Um den Amazon S3 S3-Pfad zu kopieren, aktivieren Sie das Kontrollkästchen vor der JSON-Datei und wählen Sie URL kopieren.
5. Erstellen Sie einen AWS CloudFormation Stack von der AWS CloudFormation Konsole aus. Weitere Informationen zum Erstellen eines AWS CloudFormation Stacks finden Sie unter <https://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.

Alarmer anzeigen

Sie können alle aktiven Alarmer anzeigen, die Sie zur Überwachung der Ausfallsicherheit Ihrer Anwendungen eingerichtet haben. AWS Resilience Hub verwendet eine AWS CloudFormation Vorlage zum Speichern von Alarmerdetails, die wiederum für die Erstellung der Alarmer in Amazon CloudWatch verwendet werden. Sie können über die Amazon S3 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 die Option Dashboard aus. In der Alarmtabelle 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.
- FIS läuft — Zeigt das AWS FIS Experiment an, das derzeit für Ihre Anwendung ausgeführt wird.

Um die implementierten Alarme von Anwendungen 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 für Amazon bereitgestellt wurden CloudWatch, der Status in Amazon jedoch auf INSUFFICIENT_DATA 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.
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 nicht 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 unter [the section called “Einschließlich oder ohne betriebliche Empfehlungen”](#).
- Inaktiv — Zeigt an, dass die Alarme für Amazon bereitgestellt wurden CloudWatch, der Status in Amazon jedoch auf INSUFFICIENT_DATA 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.

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 für das 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

- [Erstellung einer SOP auf der Grundlage von AWS Resilience Hub Empfehlungen](#)
- [Ein benutzerdefiniertes SSM-Dokument erstellen](#)
- [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, an die eine Ausfallsicherheitsrichtlinie angehängt 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 zum 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 unter <https://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 (AppComponent) an, die dieser SOP zugeordnet sind. Weitere Informationen zu den unterstützten AppComponent Ressourcen finden Sie unter [Ressourcen in einem AppComponent gruppieren](#).
- Referenz-ID — Gibt den logischen Bezeichner des AWS CloudFormation Stack-Ereignisses in anAWS CloudFormation.
- Empfehlungs-ID — Gibt den logischen Bezeichner der AWS CloudFormation Stack-Ressource in anAWS CloudFormation.

Experimente mit dem Amazon Fault Injection Service

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 Alarmer 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 [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.

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

- 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 unter <https://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 Experimententabelle 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 AppComponent 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 unter [the 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 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 FISaws : 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).

Grundlegendes zu Resilienzwerten

In diesem Abschnitt wird beschrieben, wie die Anwendungsbereitschaft aus verschiedenen Unterbrechungsszenarien AWS Resilience Hub quantifiziert.

AWS Resilience Hub bietet einen Resilienzwert, der die Resilienzlage der Anwendung darstellt. Dieser Wert gibt an, wie genau die Anwendung unsere Empfehlungen zur Einhaltung der Resilienzrichtlinie, Alarme, Standardbetriebsverfahren (SOPs und Tests der Anwendung befolgt. Basierend auf der Art der Ressourcen, die die Anwendung verwendet, AWS Resilience Hub empfiehlt Alarme, SOPs und eine Reihe von Tests für jeden Unterbrechungstyp.

Der höchste Resilienzwert beträgt 100 Punkte. Um den bestmöglichen Wert oder den höchsten Wert zu erreichen, müssen Sie alle empfohlenen Alarme, SOPs und Tests in Ihrer Anwendung implementieren. Zum Beispiel AWS Resilience Hub empfiehlt einen Test mit einem Alarm und einem Bol. Der Test führt den Alarm aus und löst ihn aus und initiiert den zugehörigen Bol. Wenn sie erfolgreich ausgeführt werden und die Anwendung die Resilienzrichtlinie erfüllt, erhält sie einen Resilienzwert nahe oder gleich 100 Punkten.

Nach der ersten Bewertung AWS Resilience Hub bietet eine Option zum Ausschließen betrieblicher Empfehlungen aus Ihrer Anwendung. Um die Auswirkungen der ausgeschlossenen Empfehlungen auf den Resilienzwert zu verstehen, müssen Sie eine neue Bewertung durchführen. Sie können jedoch immer die ausgeschlossenen Empfehlungen in Ihre Anwendung aufnehmen und eine neue Bewertung durchführen. Weitere Informationen zum Ein- und Ausschließen von Alarm-, Bol- und Testempfehlungen finden Sie unter [the section called “Einschließlich oder ohne betriebliche Empfehlungen”](#).

Zugriff auf den Resilienzwert Ihrer Anwendungen

Sie können den Resilienzwert Ihrer Anwendung anzeigen, indem Sie im Navigationsmenü Dashboard oder Anwendungen auswählen.

Zugriff auf den Resilienzwert über das Dashboard

1. Wählen Sie im linken Navigationsmenü Dashboard aus.
2. Wählen Sie unter Application Resiliency Score im Laufe der Zeit eine oder mehrere Anwendungen in der Dropdown-Liste Bis zu 4 Anwendungen auswählen aus.
3. Das Resilienzbewertungsdiagramm zeigt den Resilienzwert für alle ausgewählten Anwendungen an.

Zugriff auf den Resilienzwert von Anwendungen

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

Das Diagramm mit dem Resilienzwert zeigt den Trend des Resilienzwerts Ihrer Anwendung für bis zu ein Jahr an. AWS Resilience Hub zeigt Aktionselemente, Verstöße gegen Resilienzrichtlinien und betriebliche Empfehlungen an, die behoben werden müssen, um die maximal mögliche Resilienzbewertung zu verbessern und zu erreichen, indem Folgendes verwendet wird:

- Um die Aktionselemente anzuzeigen, die zur Verbesserung und Erzielung des maximal möglichen Resilienzwerts abgeschlossen werden müssen, wählen Sie die Registerkarte Aktionselemente. Wenn diese Option ausgewählt ist, wird Folgendes AWS Resilience Hub angezeigt:
 - RTO/RPO – Gibt die Anzahl der Wiederherstellungszeiten (RTO/RPOs) an, die behoben werden müssen, um die Verstöße in der Ausfallsicherheitsrichtlinie Ihrer Anwendung zu beheben. Wählen Sie den Wert aus, um die RTO/RPO-Details im Bewertungsbericht Ihrer Anwendung anzuzeigen.
 - Alarme – Gibt die Anzahl der empfohlenen Amazon- CloudWatch Alarme an, die in Ihrer Anwendung implementiert werden müssen. Wählen Sie den Wert aus, um die Amazon- CloudWatch Alarme anzuzeigen, die im Bewertungsbericht Ihrer Anwendung behoben werden müssen.
 - SOPs – Gibt die Anzahl der empfohlenen SOPs an, die in Ihrer Anwendung implementiert werden müssen. Wählen Sie den Wert aus, um die SOPs 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 den Wert jeder Komponente anzuzeigen, die sich auf Ihren Resilienzwert auswirkt, wählen Sie Punktzahlaufschlüsselung aus. Wenn diese Option ausgewählt ist, wird Folgendes AWS Resilience Hub angezeigt:
 - RTO/RPO-Compliance – 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 RTO/RPO-Schätzungen im Bewertungsbericht Ihrer Anwendung anzuzeigen.

- Implementierte Alarme – Gibt den tatsächlichen Beitrag der implementierten Amazon-CloudWatch Alarme im Vergleich zu seinem maximal möglichen Beitrag zum Resilienzwert Ihrer Anwendung an. Wählen Sie den Wert aus, um die implementierten Amazon-CloudWatch Alarme im Bewertungsbericht Ihrer Anwendung anzuzeigen.
- Implementierte SOPs – Gibt den tatsächlichen Beitrag der implementierten SOPs im Vergleich zu seinem maximal möglichen Beitrag zum Resilienzwert Ihrer Anwendung an. Wählen Sie den Wert aus, um die implementierten SOPs im Bewertungsbericht Ihrer Anwendung anzuzeigen.
- Implementierte FIS-Experimente – zeigt den tatsächlichen Beitrag der durchgeführten Tests im Vergleich zu seinem maximal möglichen Beitrag zum Resilienzwert Ihrer Anwendung an. Wählen Sie den Wert aus, um die implementierten Tests im Bewertungsbericht Ihrer Anwendung anzuzeigen.
- Um die Verstöße gegen die Ausfallsicherheitsrichtlinie und betriebliche Empfehlungen anzuzeigen, wählen Sie den rechten Pfeil, um den Abschnitt Richtlinienverletzung und Aufschlüsselung betrieblicher Empfehlungen zu erweitern. Wenn diese Option erweitert ist, wird Folgendes AWS Resilience Hub angezeigt:
 - Verstöße gegen Ausfallsicherheitsrichtlinien – Gibt die Anzahl der Anwendungskomponenten an, die gegen die Ausfallsicherheitsrichtlinie Ihrer Anwendung verstoßen. Wählen Sie den Wert neben RTO/RPO aus, um die Details auf der Registerkarte Resilienzempfehlungen des Bewertungsberichts Ihrer Anwendung anzuzeigen.
 - Operative Empfehlungen – Gibt die operativen Empfehlungen an, die nicht implementiert oder ausgeführt wurden, um die Ausfallsicherheit Ihrer Anwendung mithilfe der Registerkarten Ausstehend und Ausgeschlossen zu verbessern. Zu den operativen Empfehlungen gehören alle Empfehlungen, die inaktiv sind, und diejenigen, die nicht implementiert wurden.

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

- Alarme – Gibt die Anzahl der empfohlenen Amazon-CloudWatch Alarme an, die implementiert werden müssen.
- SOPs – Gibt die Anzahl der empfohlenen SOPs an, 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 Ausgeschlossen. Wenn diese Option ausgewählt ist, wird Folgendes AWS Resilience Hub angezeigt:

- Alarme – Gibt die Anzahl der empfohlenen Amazon- CloudWatch Alarme an, die von Ihrer Anwendung ausgeschlossen werden.
- SOPs – Gibt die Anzahl der empfohlenen SOPs an, die von Ihrer Anwendung ausgeschlossen werden.
- FIS – Gibt die Anzahl der empfohlenen Tests an, die von Ihrer Anwendung ausgeschlossen werden.

Berechnen von Resilienzwerten

In den Tabellen in diesem Abschnitt werden die Formeln erläutert, die von verwendet werden AWS Resilience Hub , um die Bewertungskomponenten jedes Empfehlungstyps und den Resilienzwert Ihrer Anwendung zu bestimmen. Alle resultierenden Werte, die von AWS Resilience Hub für Bewertungskomponenten jedes Empfehlungstyps und den Resilienzwert Ihrer Anwendung bestimmt werden, werden auf den nächsten Punkt gerundet. Wenn beispielsweise zwei von drei Alarmen implementiert wurden, würde der Wert 13,33 ($(2/3) * 20$) Punkte betragen. Dieser Wert wird auf 13 Punkte gerundet. Weitere Informationen zu Gewichtungen, die in den Formeln innerhalb der Tabellen verwendet werden, finden Sie im [the section called “Gewichtungen der - AppComponents und - Unterbrechungstypen”](#) Abschnitt .

Einige der Bewertungskomponenten können nur über die `ScoringComponentResiliencyScore` API abgerufen werden. Weitere Informationen über diese API finden Sie unter [ScoringComponentResiliencyScore](#).

Tabellen

- [Formeln zur Berechnung der Bewertungskomponente jedes Empfehlungstyps](#)
- [Formel zur Berechnung des Resilienzvalues](#)
- [Formeln zur Berechnung des Resilienzvalues für - AppComponents und -Unterbrechungstypen](#)

In der folgenden Tabelle werden die Formeln erläutert, die von verwendet werden AWS Resilience Hub , um die Bewertungskomponente jedes Empfehlungstyps zu berechnen.

Formeln zur Berechnung der Bewertungskomponente jedes Empfehlungstyps

Bewertungskomponente	Beschreibung	Formel	Beispiel
Testabdeckung (T)	<p>Ein normalisierter Wert (0–100 Punkte) basierend auf der Anzahl der Tests, die erfolgreich implementiert und ausgeschlossen wurden, aus der Gesamtzahl der AWS Resilience Hub empfohlenen Tests.</p> <div data-bbox="367 806 761 1503" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>Note</p> <p>Um den Resilienzwert zu berechnen, müssen die empfohlenen Tests in den letzten 30 Tagen erfolgreich ausgeführt worden sein, AWS Resilience Hub damit ihn als implementiert betrachtet.</p> </div>	$T = ((\text{Total number of tests implemented}) + (\text{Total number of tests excluded})) / (\text{Total number of tests recommended})$ <p>Teile der Formel sind wie folgt:</p> <ul style="list-style-type: none"> • Gesamtzahl der konfigurierten Tests – Gibt die Gesamtzahl der Tests an, die beim Erstellen und Hochladen der AWS CloudFormation Vorlage in der AWS CloudFormation Konsole konfiguriert wurden. • Gesamtzahl der empfohlenen Tests – Gibt die von empfohlenen Tests AWS Resilience Hub basierend auf den Anwendungsressourcen an. • Gesamtzahl der ausgeschlossenen Tests – Gibt die Anzahl der empfohlenen Tests 	<p>Wenn Sie 10 implementiert und 5 Tests von 20 AWS Resilience Hub empfohlenen Tests ausgeschlossen haben, wird die Testabdeckung wie folgt berechnet:</p> $T = (10 + 5) / 20$ <p>Das heißt, T = .75 or 75 points</p>

Bewertungskomponente	Beschreibung	Formel	Beispiel
		an, die Sie aus der Anwendung ausgeschlossen haben.	

Bewertungskomponente	Beschreibung	Formel	Beispiel
Alarmabdeckung (A)	<p>Ein normalisierter Wert (0–100 Punkte) basierend auf der Anzahl der Amazon CloudWatch-Alarme, die erfolgreich implementiert und ausgeschlossen wurden, aus der Gesamtzahl der AWS Resilience Hub empfohlenen Amazon- CloudWatch Alarme.</p> <div data-bbox="367 827 760 1476" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Um den Resilienzwert zu berechnen, sollten sich die empfohlenen Alarme im Status Bereit befinden, AWS Resilience Hub damit sie als implementiert betrachtet werden können.</p> </div>	$A = \left(\frac{\text{Total number of alarms implemented} + \text{Total number of alarms excluded}}{\text{Total number of alarms recommended}} \right)$ <p>Teile der Formel sind wie folgt:</p> <ul style="list-style-type: none"> • Gesamtzahl der konfigurierten Alarme – Gibt die Gesamtzahl der Amazon- CloudWatch Alarme an, die beim Erstellen und Hochladen der AWS CloudFormation Vorlage in der AWS CloudFormation Konsole konfiguriert wurden. • Gesamtzahl der empfohlenen Alarme – Gibt die Amazon- CloudWatch Alarme an, die von AWS Resilience Hub basierend auf den Anwendungsressourcen empfohlen werden. • Gesamtzahl der ausgeschlossenen Alarme – Gibt die Anzahl der empfohlenen 	<p>Wenn Sie 10 implementiert und 5 Amazon- CloudWatch Alarme von 20 AWS Resilience Hub empfohlenen Amazon- CloudWatch Alarmen ausgeschlossen haben, wird die Abdeckung der Amazon- CloudWatch Alarme wie folgt berechnet:</p> $A = (10 + 5) / 20$ <p>Das heißt, A = .75 or 75 points</p>

Bewertungskomponente	Beschreibung	Formel	Beispiel
		en Amazon- CloudWatch Alarme an, die Sie von der Anwendung ausgeschlossen haben.	

Bewertungskomponente	Beschreibung	Formel	Beispiel
Trichterbdeckung (S)	Ein normalisierter Wert (0–100 Punkte) basierend auf der Anzahl der SOPs, die erfolgreich implementiert und ausgeschlossen wurden, aus der Gesamtzahl der AWS Resilience Hub empfohlenen SOPs	$S = \left(\frac{\text{Total number of SOPs implemented} + \text{Total number of SOPs excluded}}{\text{Total number of SOPs recommended}} \right)$ <p>Teile der Formel sind wie folgt:</p> <ul style="list-style-type: none"> • Gesamtzahl der konfigurierten SOPs – Gibt die Gesamtzahl der SOPs an, die konfiguriert werden, wenn die AWS CloudFormation Vorlage in der AWS CloudFormation Konsole erstellt und hochgeladen wird. • Gesamtzahl der empfohlenen SOPs – Gibt die von empfohlenen SOPs AWS Resilience Hub basierend auf den Anwendungsressourcen an. • Gesamtzahl der SOPs – Gibt die Anzahl der empfohlenen SOPs an, die Sie aus der 	<p>Wenn Sie 10 implementiert und 5 SOPs 20 AWS Resilience Hub empfohlenen SOPs, wird die microSD-A bdeckung wie folgt berechnet:</p> $S = (10 + 5) / 20$ <p>Das heißt, S = .75 or 75 points</p>

Bewertungskomponente	Beschreibung	Formel	Beispiel
		Anwendung ausgeschlossen haben.	

Bewertungskomponente	Beschreibung	Formel	Beispiel
RTO/RPO-Compliance (P)	Ein normalisierter Wert (0–100 Punkte), basierend auf der Anwendung, die ihre Ausfallsicherheitsrichtlinie erfüllt.	$P = \frac{\text{Total weights of disruption types meeting the application's resiliency policy}}{\text{Total weights of all disruption types}}$	<p>Wenn Ihre Anwendung Ausfallsicherheitsrichtlinie nur für die Typen Availability Zone (AZ) und Infrastrukturunterbrechung erfüllt, wird der Ausfallsicherheitsrichtlinienwert (P) wie folgt berechnet:</p> <ul style="list-style-type: none"> • Wenn Sie regionale RTO- und RPO-Ziele festgelegt haben, P wird wie folgt berechnet: $P = (20 + 30) / 100$ <p>Das heißt, P = .5 or 50 points</p> • Wenn Sie keine regionalen RTO- und RPO-Ziele festgelegt haben, P wird wie folgt berechnet:

Bewertungskomponente	Beschreibung	Formel	Beispiel
			$P = (22.22 + 33.33) / 99.9$ <p>Das heißt, P = .55 or 55 points</p>

In der folgenden Tabelle wird die Formel erläutert, die von verwendet wird AWS Resilience Hub , um den Resilienzwert für Ihre gesamte Anwendung zu berechnen.

Formel zur Berechnung des Resilienzwerts

Bewertungskomponente	Beschreibung	Formel	Beispiel
Resilienzwert für Anwendung (RS)	Ein normalisierter Resilienzwert (0–100 Punkte), der darauf basiert, dass Ihre Anwendung ihre Resilienzrichtlinie erfüllt. Der Resilienzwert pro Anwendung ist der gewichtete Durchschnitt aller Empfehlungstypen. Das heißt: RS = Weighted Average (T, A, S, P)	Der Resilienzwert pro Anwendung wird mit 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 der Abdeckung jeder Empfehlungstypentabelle lauten wie folgt: <ul style="list-style-type: none"> • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5

Bewertungskomponente	Beschreibung	Formel	Beispiel
			<p>Der Resilienzwert pro Anwendung wird wie folgt berechnet:</p> $RS = ((.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .4)$ <p>Das heißt, RS = .65 or 65 points</p>

In der folgenden Tabelle werden die Formeln erläutert, die von verwendet werden AWS Resilience Hub , um den Resilienzwert für Anwendungskomponenten (AppComponents) und Unterbrechungstypen zu berechnen. Sie können den Resilienzwert der Unterbrechungstypen AppComponentents und jedoch nur über die folgenden AWS Resilience Hub-APIs abrufen:

- [DescribeAppAssessment](#) , um zu erhalten RSo
- [ListAppComponentCompliances](#) , um RSao und zu erhalten RSA

Formeln zur Berechnung des Resilienzwerths für - AppComponentents und -Unterbrechungstypen

Bewertungskomponente	Beschreibung	Formel	Beispiel
Resilienzwert pro AppComponent und pro	Ein normalisierter Wert (0–100 Punkte), basierend	Der Resilienzwert pro AppComponent und pro Unterbrechungstyp wird mit der folgenden Formel berechnet:	RSao Die Annahmen für alle Empfehlungstypen lauten wie folgt:

Bewertungskomponente	Beschreibung	Formel	Beispiel
Unterbrechungstyp (RSao)	<p>auf der AppComponent Erfüllung der Ausfallsicherheitsrichtlinie pro Unterbrechungstyp. Der Resilienzwert pro AppComponent und pro Unterbrechungstyp ist der gewichtete Durchschnitt aller Empfehlungstypen.</p> <p>Das heißt: $RSao = \text{Weighted Average (T, A, S, P)}$</p> <p>Die -Werte für T, A, S, P werden für alle empfohlenen Tests, Alarme, SOPs und die Einhaltung der Resilienz</p>	$RSao = (T * \text{Weight}(T) + A * \text{Weight}(A) + S * \text{Weight}(S) + P * \text{Weight}(P)) / (\text{Weight}(T) + \text{Weight}(A) + \text{Weight}(S) + \text{Weight}(P))$	<ul style="list-style-type: none"> • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 <p>Der Resilienzwert pro AppComponent und Unterbrechungstyp wird wie folgt berechnet:</p> $RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)$ <p>Das heißt, RSao = .65 or 65 points</p>

Bewertungskomponente	Beschreibung	Formel	Beispiel
	richtlinie des AppComponent und des Unterbrechungstyps berechnet.		

Bewertungskomponente	Beschreibung	Formel	Beispiel
Resilienzwert pro AppComponent (RSa)	<p>Ein normalisierter Wert (0–100 Punkte), basierend auf der Erfüllung seiner Ausfallsicherheitsrichtlinie. Der Resilienzwert pro AppComponent ist der gewichtete Durchschnitt aller Empfehlungstypen. Das heißt: RSa = Weighted Average (T, A, S, P)</p> <p>Die Werte für T, A, S, P werden für alle empfohlenen Tests, Alarme, SOPs und die Einhaltung der Resilienzrichtlinie des berechnet</p>	<p>Der Resilienzwert pro AppComponent wird mit der folgenden Formel berechnet:</p> $RSa = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))$	<p>RSa Die Annahmen für alle Empfehlungstypen lauten wie folgt:</p> <ul style="list-style-type: none"> • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 <p>Der Resilienzwert pro AppComponent wird wie folgt berechnet:</p> $RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)$ <p>Das heißt, RSa = .65 or 65 points</p>

Bewertungskomponente	Beschreibung	Formel	Beispiel
	AppCompon ent.		

Bewertungskomponente	Beschreibung	Formel	Beispiel
Resilienzwert pro Unterbrechungstyp (RSo)	<p>Ein normalisierter Wert (0–100 Punkte), basierend auf der Erfüllung seiner Ausfallsicherheitsrichtlinie. Der Resilienzwert pro Unterbrechungstyp ist der gewichtete Durchschnitt aller Empfehlungstypen. Das heißt: $RSo = \text{Weighted Average (T, A, S, P)}$</p> <p>Die Werte für T, A, S, P werden für alle empfohlenen Tests, Alarme, SOPs und die Einhaltung der Ausfallsicherheitsrichtlinie des -Unterbre</p>	<p>Der Resilienzwert pro Unterbrechungstyp wird mit der folgenden Formel berechnet:</p> $RSo = (T * \text{Weight}(T) + A * \text{Weight}(A) + S * \text{Weight}(S) + P * \text{Weight}(P)) / (\text{Weight}(T) + \text{Weight}(A) + \text{Weight}(S) + \text{Weight}(P))$	<p>RSo Die Annahmen für alle Empfehlungstypen lauten wie folgt:</p> <ul style="list-style-type: none"> • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 <p>Der Resilienzwert pro Unterbrechungstyp wird wie folgt berechnet:</p> $RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)$ <p>Das heißt, $RSo = .65$ or 65 points</p>

Bewertungskomponente	Beschreibung	Formel	Beispiel
	chungstyps berechnet.		

Gewichtungen

AWS Resilience Hub weist jedem Empfehlungstyp eine Gewichtung für den gesamten Resilienzwert zu.

Die folgenden Tabellen zeigen die Gewichtung für Alarme, SOPs Tests, Einhaltung von Resilienzrichtlinien und Unterbrechungstypen. Der Unterbrechungstyp umfasst Anwendung, Infrastruktur, AZ und Region.

Note

Wenn Sie keine regionalen RTO- oder RPO-Ziele für Ihre Richtlinie definieren möchten, werden die Gewichtungen für die anderen Unterbrechungstypen entsprechend erhöht, wie unter Gewicht, wenn Region nicht definiert ist Spalte.

Gewichtungen für Alarme, SOPs Tests, Richtlinienziel

Empfehlungstyp	Gewicht
Alarme	20 Punkte
SOPs	20 Punkte
Tests	20 Punkte
Richtlinie für die Einhaltung der Ausfallsicherheit	40 Punkte

Gewichtungen für den Unterbrechungstyp

Unterbrechungstyp	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 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" : {

"ReadThrottleEventThresholdExceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm" :
{
  "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 Weg, einen Alarm, eine SOP 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 Datei im JSON-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 Anwendungstapeln 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}:
\u0026lbrace;\u0026lbrace;ReadThrottleEventThresholdExceededDynamoDBEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
\u0026lbrace;referenceId\u0026lbrace;:\u0026lbrace;dynamodb:alarm:health_read_throttle_events:2020-04-01\u0026lbrace;\",
\u0026lbrace;resourceId\u0026lbrace;:\u0026lbrace;Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\u0026lbrace;,\u0026lbrace;relatedSOPs\u0026lbrace;\":
[\u0026lbrace;dynamodb:sop:update_provisioned_capacity:2020-04-01\u0026lbrace;]}\u0026lbrace;}"
```

zum Folgenden:

```
"Fn::Sub" : "${alarmName}:
\u0026lbrace;\u0026lbrace;ReadThrottleEventThresholdExceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm\u0026lbrace;}\u0026lbrace;\",
\u0026lbrace;referenceId\u0026lbrace;:\u0026lbrace;dynamodb:alarm:health_read_throttle_events:2020-04-01\u0026lbrace;,\u0026lbrace;resourceId
\u0026lbrace;:\u0026lbrace;${Employees}\u0026lbrace;,\u0026lbrace;relatedSOPs\u0026lbrace;\":
[\u0026lbrace;dynamodb:sop:update_provisioned_capacity:2020-04-01\u0026lbrace;]}\u0026lbrace;}"
```

Beim Ändern von AWS CloudFormation Vorlagen für SOPs und AWS FIS Experimente verwenden Sie denselben Ansatz und ersetzen hartcodierte Referenz-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 zur 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.

Verwendung von AWS Resilience Hub APIs zur Beschreibung und Verwaltung von Anwendungen

Als Alternative zur Beschreibung und Verwaltung von Anwendungen mithilfe der AWS Resilience Hub Konsole AWS Resilience Hub können Sie Anwendungen mithilfe von AWS Resilience Hub APIs beschreiben und verwalten. In diesem Kapitel wird erklärt, wie eine Anwendung mithilfe von AWS Resilience Hub APIs erstellt wird. Es definiert auch die Reihenfolge, in der Sie die APIs ausführen müssen, 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: Vorbereiten 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 zu erstellen AWS Resilience Hub, müssen Sie die CreateApp API aufrufen und einen eindeutigen Anwendungsnamen angeben. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

Das folgende Beispiel zeigt, wie Sie AWS Resilience Hub mithilfe der CreateApp API eine neue Anwendung newApp erstellen.

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 Resilienzrichtlinie erstellen, die es Ihnen ermöglicht, den Ausfallsicherheitsstatus Ihrer Anwendung mithilfe CreateResiliencyPolicy der API zu verstehen. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html.

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

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 die folgenden APIs zum Importieren von Ressourcen in Ihre Anwendung:

- **ImportResourcesToDraftAppVersion**— Diese API ermöglicht es Ihnen, Ressourcen aus verschiedenen Eingabequellen in die Entwurfsversion Ihrer Anwendung zu importieren. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- **PublishAppVersion**— Diese API veröffentlicht zusammen mit der aktualisierten Version eine neue Version der Anwendung AppComponents. Weitere Informationen über diese

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

- `DescribeDraftAppVersionResourcesImportStatus`— Mit dieser API können Sie den Importstatus Ihrer Ressourcen in eine Anwendungsversion überwachen. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

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

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 AWS Resilience Hub mithilfe der `CreateAppVersionResource` API manuell Ressourcen hinzufügen können.

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 Ressourcen AWS Resilience Hub mithilfe der `DescribeDraftAppVersionResourcesImportStatus` API überwachen können.

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. Verwenden Sie die `PublishAppVersion` API, um die Entwurfsversion Ihrer Anwendung zu veröffentlichen. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

Das folgende Beispiel zeigt, wie Sie die Entwurfsversion der Anwendung AWS Resilience Hub mithilfe der `PublishAppVersion` API veröffentlichen.

Anforderung

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

Antwort

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

2. Wenden Sie mithilfe der `UpdateApp` API eine Resilienzrichtlinie auf die veröffentlichte Version Ihrer Anwendung an. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html.

Das folgende Beispiel zeigt, wie Sie AWS Resilience Hub mithilfe UpdateApp der API eine Resilienzrichtlinie auf die veröffentlichte Version einer Anwendung anwenden.

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 den geschätzten Workload-RTO und den geschätzten RPO-Wert erfüllt, die in Ihrer Resilienzrichtlinie definiert sind. Bei der Bewertung wird jede Konfiguration der Anwendungskomponente mit der Richtlinie verglichen und es werden Alarm-, SOP- und 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 die folgenden APIs verwenden:

- `StartAppAssessment`— Diese API erstellt eine neue Bewertung für eine Anwendung. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.
- `DescribeAppAssessment`— Diese API beschreibt eine Bewertung für die Anwendung und gibt den Abschlussstatus der Bewertung an. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

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

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 AWS Resilience Hub mithilfe der DescribeAppAssessment API überwachen können. 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 Bewertungsergebnisse mithilfe der folgenden APIs überprüfen.

- **DescribeAppAssessment**— Mit dieser API 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 über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.
- **ListAlarmRecommendations**— Diese API ermöglicht es Ihnen, die Alarmempfehlungen mithilfe des Amazon-Ressourcennamens (ARN) der Bewertung abzurufen. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html.

Note

Verwenden `ListSopRecommendations` Sie `ListTestRecommendations` APIs, um die SOP- und FIS-Testerempfehlungen zu erhalten.

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

Note

Um die SOP- und FIS-Testempfehlungen zu erhalten, 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 CloudWatch Synthetics is setup to monitor the
application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/
monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>). \nMake
sure that the Synthetics Name passed in the alarm dimension matches the name of the
Synthetic Canary. It Defaults to the name of the application.\n"
    }
  ],
}
```

```

    {
      "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
      "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
      "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
      "description": "Alarm by AWS ResilienceHub that reports when EFS I/O load
is more than 90% for too much time",
      "type": "Metric",
      "appComponentName": "storageappcomponent-rlb",
      "items": [
        {
          "resourceId": "fs-0487f945c02f17b3e",
          "targetAccountId": "12345678901",
          "targetRegion": "us-west-2",
          "alreadyImplemented": false
        }
      ]
    },
    {
      "recommendationId": "09f340cd-3427-4f66-8923-7f289d4a3216",
      "referenceId": "efs:alarm:mount_failure:2020-04-01",
      "name": "AWSResilienceHub-EFSMountFailureAlarm_2020-04-01",
      "description": "Alarm by AWS ResilienceHub that reports when volume failed
to mount to EC2 instance",
      "type": "Metric",
      "appComponentName": "storageappcomponent-rlb",
      "items": [
        {
          "resourceId": "fs-0487f945c02f17b3e",
          "targetAccountId": "12345678901",
          "targetRegion": "us-west-2",
          "alreadyImplemented": false
        }
      ],
      "prerequisite": "* Make sure Amazon EFS utils are installed(see the <a
href=\"https://github.com/aws/efs-utils#installation\" target=\"_blank\">docs</a>).
\n* Make sure cloudwatch logs are enabled in efs-utils (see the <a href=\"https://
github.com/aws/efs-utils#step-2-enable-cloudwatch-log-feature-in-efs-utils-config-
file-etcamazonefsefs-utilsconf\" target=\"_blank\">docs</a>).\n* Make sure that
you've configured `log_group_name` in `/etc/amazon/efs/efs-utils.conf`, for example:
`log_group_name = /aws/efs/utils`.\n* Use the created `log_group_name` in the
generated alarm. Find `LogGroupName: REPLACE_ME` in the alarm and make sure the
`log_group_name` is used instead of REPLACE_ME.\n"
    },
  ]
}

```

```
    "recommendationId": "b0f57d2a-1220-4f40-a585-6dab1e79cee2",
    "referenceId": "efs:alarm:client_connections:2020-04-01",
    "name": "AWSResilienceHub-EFSHighClientConnectionsAlarm_2020-04-01",
    "description": "Alarm by AWS ResilienceHub that reports when client
connection number deviation is over the specified threshold",
    "type": "Metric",
    "appComponentName": "storageappcomponent-rlb",
    "items": [
      {
        "resourceId": "fs-0487f945c02f17b3e",
        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
        "alreadyImplemented": false
      }
    ]
  },
  {
    "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
    "referenceId": "rds:alarm:health-storage:2020-04-01",
    "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
    "description": "Reports when database free storage is low",
    "type": "Metric",
    "appComponentName": "databaseappcomponent-hji",
    "items": [
      {
        "resourceId": "terraform-20220623141426115800000001",
        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
        "alreadyImplemented": false
      }
    ]
  },
  {
    "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
    "referenceId": "rds:alarm:health-connections:2020-04-01",
    "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
    "description": "Reports when database connection count is anomalous",
    "type": "Metric",
    "appComponentName": "databaseappcomponent-hji",
    "items": [
      {
        "resourceId": "terraform-20220623141426115800000001",
        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
```

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

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

```

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

```

Das folgende Beispiel zeigt, wie Sie mithilfe der ListAppComponentRecommendations API die Konfigurationsempfehlungen (Empfehlungen zur Verbesserung Ihrer aktuellen Resilienz) abrufen können.

Anforderung

```

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

```

Antwort

```

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

```

```

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

```

```

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

```

```

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

```

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

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

```
"cost": {
  "amount": 76.73,
  "currency": "USD",
  "frequency": "Monthly"
},
"appComponentName": "databaseappcomponent-hji",
"recommendationCompliance": {
  "AZ": {
    "expectedComplianceStatus": "PolicyMet",
    "expectedRtoInSecs": 120,
    "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
    "expectedRpoInSecs": 0,
    "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
  },
  "Hardware": {
    "expectedComplianceStatus": "PolicyMet",
    "expectedRtoInSecs": 120,
    "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
    "expectedRpoInSecs": 0,
    "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
  },
  "Software": {
    "expectedComplianceStatus": "PolicyMet",
    "expectedRtoInSecs": 900,
    "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
    "expectedRpoInSecs": 300,
    "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
  }
},
"optimizationType": "BestAZRecovery",
"description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
"suggestedChanges": [
  "Add read replica in the same region",
  "Change DB instance to a supported class (db.t3.small)",
  "Change to Aurora",
  "Enable cluster backtracking",
  "Enable instance backup with retention period 7"
```

```

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

```

```

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

```

```
        "referenceId": "efs:config:with_backups:2020-04-01"  
      }  
    ]  
  }  
]
```

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 AppComponentent”](#)

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 der `CreateAppVersionResource` API manuell zu Ihrer Anwendung hinzufügen. Weitere Informationen über diese API finden Sie unter https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

Sie müssen die folgenden Parameter für diese API angeben:

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

Das folgende Beispiel zeigt, wie Sie Ihrer Anwendung AWS Resilience Hub mithilfe der `CreateAppVersionResource` API manuell Ressourcen hinzufügen können.

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, AppComponent mithilfe der folgenden Ressourcenverwaltungs-APIs Ressourcen zu einer einzigen zu gruppieren.

- `UpdateAppVersionResource`— Diese API aktualisiert die Ressourcendetails einer Anwendung. Weitere Informationen über diese API finden Sie unter [UpdateAppVersionResource](#).
- `DeleteAppVersionAppComponent`— Diese API löscht die AppComponent aus der Anwendung. Weitere Informationen über diese API finden Sie unter [DeleteAppVersionAppComponent](#).

Das folgende Beispiel zeigt, wie Sie die Ressourcendetails Ihrer Anwendung AWS Resilience Hub mithilfe der `DeleteAppVersionAppComponent` API aktualisieren.

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 Beispielen AWS Resilience Hub mithilfe der `UpdateAppVersionResource` API erstellt wurde.

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 mithilfe der `UpdateAppVersionResource` API von Bewertungen auszuschließen. Diese Ressourcen werden bei der Berechnung der Ausfallsicherheit Ihrer Anwendung nicht berücksichtigt. Weitere Informationen über diese API finden Sie unter https://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 Ihrer Anwendung bei der AWS Resilience Hub Verwendung der `UpdateAppVersionResource` API ausschließen können.

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](#)
- [Identity and Access Management für AWS Resilience Hub](#)
- [Sicherheit der Infrastruktur in AWS Resilience Hub](#)

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 unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie 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 zu schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS benötigt TLS 1.2 und empfiehlt TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. 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 für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

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 arbeiten und die Konsole, die API oder SDKs AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

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 Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um AWS Resilience Hub-Ressourcen zu nutzen. IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert AWS Resilience Hub mit IAM](#)
- [Richten Sie IAM-Rollen und -Berechtigungen ein](#)
- [Fehlerbehebung bei Identität und Zugriff auf AWS Resilience Hub](#)
- [AWS Resilience Hub Referenz zu Zugriffsberechtigungen](#)
- [AWS verwaltete Richtlinien für AWS Resilience Hub](#)
- [Die Terraform-Statusdatei wird importiert in AWS Resilience Hub](#)
- [AWS Resilience Hub Zugriff auf Ihren Amazon Elastic Kubernetes Service Service-Cluster aktivieren](#)

- [Aktivierung AWS Resilience Hub der Veröffentlichung in Ihren Amazon Simple Notification Service-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 Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie auf eine Funktion in AWS Resilience Hub nicht zugreifen können, finden Sie weitere Informationen unter [Fehlerbehebung 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. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit AWS Resilience Hub nutzen kann, finden Sie unter [So funktioniert AWS Resilience Hub mit IAM](#).

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Resilience Hub zu AWS zu verwalten. Beispiele für identitätsbasierte AWS Resilience Hub-Richtlinien, die Sie in IAM verwenden können, 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 annehmen. 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 (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportale 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 denen 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 IAM-Benutzerhandbuch 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 \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, 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 unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

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 [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) 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 einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten 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 [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. 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 oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **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 unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, 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 andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- **Kontoübergreifender Zugriff** – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal 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 zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.
- **Serviceübergreifender Zugriff** — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann

dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.

- **Forward Access Sessions (FAS)** — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services können Sie Aktionen ausführen, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen 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 für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- **Servicerolle** – Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- **Dienstbezogene Rolle** — Eine dienstbezogene 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 Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Auf Amazon EC2 ausgeführte Anwendungen** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren 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 AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

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 und einer eingebundenen Richtlinie

wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-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 von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter [Zugriffskontrollliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

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 ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen 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 über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.

- **Service Control Policies (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter [Funktionsweise von SCPs](#) 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 unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

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 IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

So funktioniert AWS Resilience Hub mit IAM

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

IAM-Funktionen, die Sie mit Resilience Hub verwenden können AWS

IAM-Feature	AWS Resilience Hub-Unterstützung
Identitätsbasierte Richtlinien	Ja

IAM-Feature	AWS Resilience Hub-Unterstützung
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Resilience Hub und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

Identitätsbasierte Richtlinien für Resilience Hub AWS

Unterstützt Richtlinien auf Identitätsbasis.	Ja
--	----

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer

identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Maßnahmen für Resilience Hub AWS

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 an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-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 kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie 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 erteilen. 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 unter [Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden](#) im IAM-Benutzerhandbuch.

Politische Maßnahmen für AWS Resilience Hub

Unterstützt Richtlinienaktionen	Ja
---------------------------------	----

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

Das Element `Action` 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, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. 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 angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. 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 ARNs finden Sie unter [Von AWS Resilience Hub definierte Ressourcen](#) in der Serviceautorisierungsreferenz. Informationen zu den Aktionen, mit denen Sie den ARN jeder Ressource angeben 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 auf was Zugriff 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. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

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](#)

ACLs im Resilience Hub AWS

Unterstützt ACLs

Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Resilience Hub AWS

Unterstützt ABAC (Tags in Richtlinien)

Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden 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 von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement 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 ABAC finden Sie unter [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Verwendung temporärer Anmeldeinformationen mit AWS Resilience Hub

Unterstützt temporäre Anmeldeinformationen	Ja
--	----

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#), finden Sie im [IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort 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 Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. 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 in IAM](#).

Zugriffssitzungen für AWS Resilience Hub weiterleiten

Unterstützt Forward Access Sessions (FAS)	Ja
---	----

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services können Sie Aktionen ausführen, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen 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 für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für AWS Resilience Hub

Unterstützt Servicerollen	Ja
---------------------------	----

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

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 der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS Resilience Hub definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resilience Hub](#) in der Referenz zur Serviceautorisierung.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der Resilience Hub-Konsole AWS](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Verfügbare Anwendungen auflisten AWS Resilience Hub](#)
- [Starten einer Anwendungsbeurteilung](#)
- [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 unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung 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 von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Resilience Hub-Konsole AWS

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 die AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer 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 unter [Hinzufügen von Berechtigungen zu einem Benutzer](#) im IAM-Benutzerhandbuch.

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

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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 Anwendungsbeurteilung

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/*" }
      }
    }
  ]
}
```

```
]
}
```

Richten Sie IAM-Rollen und -Berechtigungen ein

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 schreibgeschützten Zugriff 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 `AwsResilienceHubAssessmentPolicy` 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 Rollename in den anderen Konten verwendet, um auf die kontoübergreifenden Ressourcen zuzugreifen. Optional können Sie die Rollen-ARNs für andere Konten konfigurieren, die anstelle des Rollennamens des Aufrufers verwendet werden.

- Aktueller IAM-Benutzerzugriff — AWS Resilience Hub verwendet den aktuellen IAM-Benutzer für den Zugriff auf Ihre Anwendungsressourcen. Wenn sich Ihre Ressourcen in einem anderen Konto befinden, AWS Resilience Hub übernimmt er die folgenden IAM-Rollen für den Zugriff auf die Ressourcen:
 - `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. die Erkennung von Resilienzabweichungen) 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 IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion in AWS Resilience Hub durchzuführen](#)
- [Ich bin nicht berechtigt, iam auszuführen: 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 IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `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 auszuführen: 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. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, 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 [So 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 für einen IAM-Benutzer in einem anderen AWS-Konto, den Sie besitzen](#).

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

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 anhängen, 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 von [the 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 "Verwenden der IAM-Rolle"](#)

- [the section called “Aktuelle IAM-Benutzerberechtigungen verwenden”](#)

Verwenden Sie die IAM-Rolle

AWS Resilience Hub verwendet eine vordefinierte bestehende 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 den Zugriff auf AWS Dienste und Ressourcen AWS Resilience Hub voraussetzt. 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 Anwendungsaufuferrolle.

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 Anwendungsaufuferrolle 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 IAM-Konsole erstellen”](#)
- [the section called “Verwalten von Rollen mit der IAM-API”](#)
- [the section called “Definition der Vertrauensrichtlinie mithilfe der JSON-Datei”](#)

Eine Aufruferrolle in der IAM-Konsole erstellen

Um den Zugriff auf AWS Dienste und Ressourcen AWS Resilience Hub zu ermöglichen, müssen Sie mithilfe der IAM-Konsole eine Aufruferrolle im primären Konto erstellen. 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 der IAM-Konsole eine Aufruferrolle im primären Konto

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
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“ **AWSResilienceHubAssessmentExecutionPolicy** 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 (Rolle erstellen) 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

Wenn Sie die Anwendung erstellen oder aktualisieren, benötigen Sie in Ihrem aktuellen IAM-Benutzer/Ihrer aktuellen IAM-Rolle eine `iam:passRole` Berechtigung für die Aufruferrolle. Sie benötigen diese Berechtigung jedoch nicht, um eine Bewertung durchzuführen.

Verwalten von Rollen mit der 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. Während Sie diesen Befehl verwenden, 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 der Vertrauensrichtlinie mithilfe der 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-role` Befehl, um der Rolle Berechtigungen hinzuzufügen, und Sie können damit beginnen, die `AWSResilienceHubAssessmentExecutionPolicy` verwaltete Richtlinie hinzuzufügen. Weitere Informationen zu dieser verwalteten Richtlinie finden Sie unter [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

Beispiel **trust-policy.json**

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

Probe **create-role**

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

Beispielausgabe

```
{
  "Role": {
    "Path": "/",
    "RoleName": "AWSResilienceHubAssessmentRole",
    "RoleId": "AROAQFOX MPL6TZ6ITKWND",
    "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/
AWSResilienceHubAssessmentExecutionPolicy
```

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 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

- [the section called “In der IAM-Konsole eine Rolle für Sekundär-/Ressourcenkonten erstellen”](#)
- [the section called “Verwalten von Rollen mit der IAM-API”](#)
- [the section called “Definition der Vertrauensrichtlinie mithilfe der JSON-Datei”](#)

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 Rollen in jedem dieser Konten erstellen.

Um mithilfe der IAM-Konsole eine Rolle in der IAM-Konsole für die sekundären Konten bzw. Ressourcenkonten zu erstellen

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen und anschließend 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“ **AWSResilienceHubAssessmentExecutionPolicy** 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 (Rolle erstellen) 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"
  ]
}
```

Verwalten von Rollen mit der 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 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": {"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 der 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-role` Befehl, um einer Rolle Berechtigungen hinzuzufügen, und Sie können damit beginnen, die `AWSResilienceHubAssessmentExecutionPolicy` verwaltete Richtlinie hinzuzufügen. Weitere Informationen zu dieser verwalteten Richtlinie finden Sie unter [the section called "AWSResilienceHubAssessmentExecutionPolicy"](#).

Beispiel trust-policy.json

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

```

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

```

Probe **create-role**

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

Beispielausgabe

```

{
  "Role": {
    "Path": "/",
    "RoleName": "AWSResilienceHubAssessmentRole2",
    "RoleId": "AR0AT2GICMEDJML6EVQRG",
    "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/AWSResilienceHubAssessmentExecutionPolicy.
```

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 `AWSResilienceHubAssessmentExecutionPolicy` 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 durchzuführen AWS Resilience Hub zu können.

Note

- Bei Verwendung des rollenbasierten Zugriffs (mit der oben genannten Aufruferrolle) ist dieser Schritt nicht erforderlich.
- Der Rollename muss sein. `AwsResilienceHubPeriodicAssessmentRole`

Um die Durchführung von geplanten Aufgaben im Zusammenhang mit der Bewertung AWS Resilience Hub zu ermöglichen

1. Hängen Sie die `AWSResilienceHubAssessmentExecutionPolicy` 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 Amazon EKS-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 Rollename muss sein `AwsResilienceHubAdminAccountRole`.
- Er muss im Hauptkonto erstellt werden.
- Ihr aktueller IAM-Benutzer/Ihre aktuelle IAM-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/
      "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 `AWSResilienceHubAssessmentExecutionPolicy` 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.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur

Verfügung stehen. 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 unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWSResilienceHubAssessmentExecutionPolicy

Sie können die `AWSResilienceHubAssessmentExecutionPolicy` 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 `beginnenaws-resilience-hub-artifacts-` beginnen. Wenn Sie in einem anderen Amazon S3 S3-Bucket veröffentlichen möchten, können Sie dies tun, während Sie die `CreateRecommendationTemplate` API aufrufen. 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 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 (Amazon EC2) — Listet Amazon EC2-Ressourcen auf und bietet `Describe` Berechtigungen für Amazon EC2 EC2-Ressourcen, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic Container Registry (Amazon ECR) — Stellt `Describe` Berechtigungen für Amazon ECR-Ressourcen bereit, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic Container Service (Amazon ECS) — Stellt `Describe` Berechtigungen für Amazon ECS-Ressourcen bereit, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic File System (Amazon EFS) — Stellt `Describe` Berechtigungen für Amazon EFS-Ressourcen bereit, die mit Ihrem AWS Konto verknüpft sind.
- Amazon Elastic Kubernetes Service (Amazon EKS) — Listet Amazon EKS-Ressourcen auf und bietet `Describe` Berechtigungen für Amazon EKS-Ressourcen, die mit Ihrem AWS Konto verknüpft sind.
- Amazon EC2 Auto Scaling — Listet Amazon EC2 Auto Scaling-Ressourcen auf und bietet `Describe` Berechtigungen für Amazon EC2 Auto Scaling Scaling-Ressourcen, die Ihrem AWS Konto zugeordnet sind.
- Amazon EC2 Systems Manager (SSM) — Stellt `Describe` Berechtigungen für SSM-Ressourcen bereit, die mit Ihrem Konto verknüpft sind. AWS
- 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 for Windows File Server (Amazon FSx) — Listet Amazon FSx-Ressourcen auf, die mit Ihrem Konto verknüpft sind, und gewährt `Describe` Berechtigungen für diese Ressourcen. AWS
- Amazon RDS — Listet Amazon RDS-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und bietet `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 (Amazon SNS) — Listet Amazon SNS SNS-Ressourcen auf, die mit Ihrem AWS Konto verknüpft sind, und gewährt `Describe` Berechtigungen dafür.

- Amazon Simple Queue Service (Amazon SQS) — Listet Amazon SQS SQS-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 und gewährt `Describe` Berechtigungen, die mit Ihrem AWS Konto verknüpft sind.

Note

Wenn während der Durchführung einer Bewertung Berechtigungen fehlen, die aus den verwalteten Richtlinien aktualisiert werden müssen, AWS Resilience Hub wird die Bewertung mit `s3: GetBucketLogging Permission` erfolgreich abgeschlossen. Es AWS Resilience Hub wird jedoch eine Warnmeldung angezeigt, die die fehlenden Berechtigungen auflistet und eine Frist einräumt, 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 mit Ihrem AWS Konto verknüpft 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 SOPs zu verwalten, die für Ihre Anwendung konfiguriert sind.

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 Bewertungen gewähren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",

```

```
"ec2:DescribeAvailabilityZones",
"ec2:DescribeFastSnapshotRestores",
"ec2:DescribeFleets",
"ec2:DescribeHosts",
"ec2:DescribeInstances",
"ec2:DescribeNatGateways",
"ec2:DescribePlacementGroups",
"ec2:DescribeRegions",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ecr:DescribeRegistry",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeContainerInstances",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:ListContainerInstances",
"ecs:ListServices",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodegroup",
"eks:ListFargateProfiles",
"eks:ListNodegroups",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeSnapshots",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"fis:GetExperimentTemplate",
"fis:ListExperimentTemplates",
"fis:ListExperiments",
"fsx:DescribeFileSystems",
"lambda:GetFunctionConcurrency",
"lambda:GetFunctionConfiguration",
"lambda:ListAliases",
```

```
"lambda:ListVersionsByFunction",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyTargets",
"rds:DescribeDBSnapshots",
"rds:DescribeGlobalClusters",
"resource-groups:GetGroup",
"resource-groups:ListGroupResources",
"route53-recovery-control-config:ListClusters",
"route53-recovery-control-config:ListControlPanels",
"route53-recovery-control-config:ListRoutingControls",
"route53-recovery-readiness:GetReadinessCheckStatus",
"route53-recovery-readiness:GetResourceSet",
"route53-recovery-readiness:ListReadinessChecks",
"route53:GetHealthCheck",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53:ListResourceRecordSets",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverEndpointIpAddresses",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketPolicyStatus",
"s3:GetBucketTagging",
"s3:GetBucketVersioning",
"s3:GetMultiRegionAccessPointRoutes",
"s3:GetReplicationConfiguration",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListMultiRegionAccessPoints",
"servicecatalog:GetApplication",
"servicecatalog:ListAssociatedResources",
"sns:GetSubscriptionAttributes",
"sns:GetTopicAttributes",
"sns:ListSubscriptionsByTopic",
"sqs:GetQueueAttributes",
"sqs:GetQueueUrl",
"ssm:DescribeAutomationExecutions",
"states:DescribeStateMachine",
"states:ListStateMachineVersions",
```

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

```
]
}
```

AWS Resilience Hub Aktualisierungen der verwalteten AWS 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 — AWS Resilience Hub erweitert die Unterstützung für Amazon FSx for Windows File Server.	Diese AWS Resilience Hub Richtlinie ermöglicht es Ihnen, die Amazon FSx for Windows File Server Server-Konfiguration zu lesen.	26. März 2024
AWSResilienceHubAssessmentExecutionPolicy — AWS Resilience Hub erweitert die Unterstützung für AWS Step Functions.	Diese AWS Resilience Hub Richtlinie ermöglicht es Ihnen, die AWS Step Functions Konfiguration zu lesen.	30. Oktober 2023
AWSResilienceHubAssessmentExecutionPolicy — AWS Resilience Hub verbessert die Unterstützung für Amazon Relational Database Service (Amazon RDS).	Diese AWS Resilience Hub Richtlinie ermöglicht Ihnen den Zugriff auf Ressourcen in Amazon RDS, während Sie Bewertungen durchführen.	05. Oktober 2023
AWSResilienceHubAssessmentExecutionPolicy – Neue Richtlinie.	Diese AWS Resilience Hub Richtlinie ermöglicht den Zugriff auf andere AWS Dienste für die Durchführung von Bewertungen.	26. Juni 2023

Änderung	Beschreibung	Datum
AWS Resilience Hub hat begonnen, Änderungen zu verfolgen	AWS Resilience Hub hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	15. Juni 2023

Die Terraform-Statusdatei wird importiert 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 (SSE-KMS) verschlüsselt wurden. Wenn Ihre Terraform-Statusdateien mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C) verschlüsselt sind, können Sie sie nicht importieren. AWS Resilience Hub

Für den Import von Terraform-Statusdateien in sind die folgenden IAM-Richtlinien AWS Resilience Hub erforderlich, je nachdem, wo sich Ihre Statusdatei befindet.

Terraform-Statusdateien aus einem Amazon S3 S3-Bucket importieren, der sich im Hauptkonto befindet

Die folgende Amazon S3 S3-Bucket-Richtlinie und die IAM-Richtlinie 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 `AWSResilienceHubAssessmentExecutionPolicy` verwaltete Richtlinie verwenden, ist keine `ListBucket` Genehmigung erforderlich.

Note

Wenn Ihre Terraform-Statusdateien mit KMS verschlüsselt sind, 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 Kontrolle, 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 `AWSResilienceHubAssessmentExecutionPolicy` verwaltete Richtlinie verwenden, ist keine `ListBucket` Genehmigung erforderlich.

Note

Wenn Ihre Terraform-Statusdateien mit KMS verschlüsselt sind, 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 (Amazon EKS) -Clusters, indem die Infrastruktur Ihres Amazon EKS-Clusters analysiert wird. AWS Resilience Hub verwendet die RBAC-Konfiguration (Role Based Access Control) von Kubernetes, um andere Kubernetes-Workloads (K8s) zu bewerten, die als Teil des Amazon EKS-Clusters bereitgestellt werden. Um Ihren Amazon EKS-Cluster zur Analyse und Bewertung der Arbeitslast abzufragen, müssen Sie die folgenden Schritte ausführen:

- Erstellen oder verwenden Sie eine bestehende AWS Identity and Access Management (IAM) Rolle in demselben Konto wie der Amazon EKS-Cluster.
- Aktivieren Sie den IAM-Benutzer- und Rollenzugriff auf Ihren Amazon EKS-Cluster und gewähren Sie zusätzliche Nur-Lese-Berechtigungen für K8s-Ressourcen innerhalb des Amazon EKS-Clusters. Weitere Informationen zur Aktivierung des IAM-Benutzer- und Rollenzugriffs auf Ihren Amazon EKS-Cluster finden Sie unter [Aktivieren des IAM-Benutzer- und Rollenzugriffs auf Ihren Cluster — Amazon EKS](#).

Der Zugriff auf Ihren Amazon EKS-Cluster mithilfe von IAM-Entitäten wird durch den [AWS IAM Authenticator for Kubernetes](#) ermöglicht, der auf der Amazon EKS-Steuerebene ausgeführt wird. Der Authenticator bezieht die Konfigurationsinformationen von `aws-auth ConfigMap`

Note

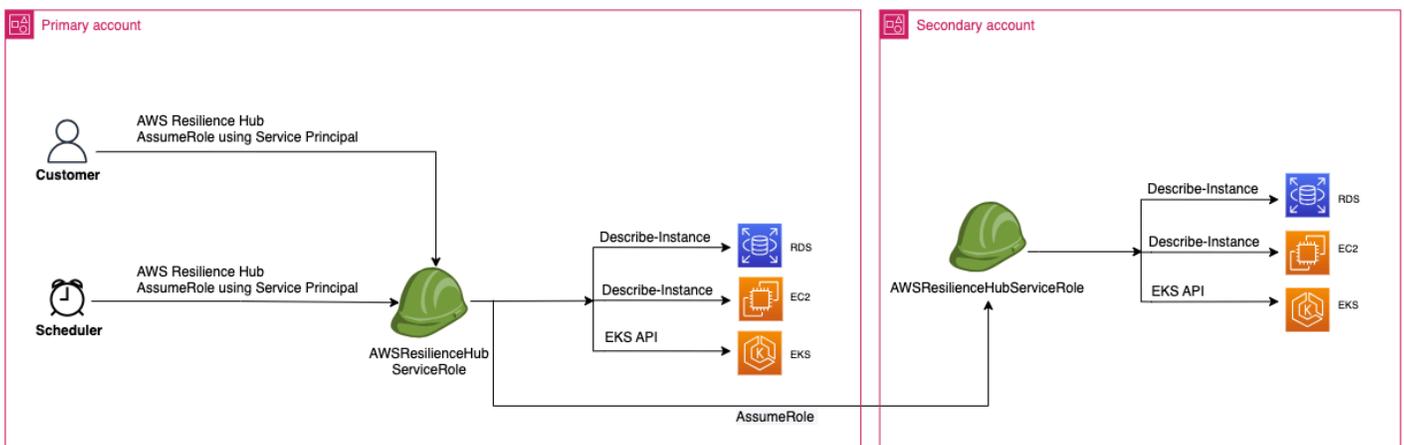
- Weitere Informationen zu allen `aws-auth` ConfigMap Einstellungen finden Sie unter [Vollständiges Konfigurationsformat](#) unter. GitHub
- Weitere Informationen zu verschiedenen IAM-Identitäten finden Sie unter [Identitäten \(Benutzer, Gruppen und Rollen\)](#) im IAM-Benutzerhandbuch.
- [Weitere Informationen zur Konfiguration der rollenbasierten Zugriffskontrolle \(RBAC\) von Kubernetes finden Sie unter Verwenden der RBAC-Autorisierung.](#)

AWS Resilience Hub fragt Ressourcen in Ihrem Amazon EKS-Cluster mithilfe einer IAM-Rolle in Ihrem Konto ab. Damit Sie AWS Resilience Hub auf Ressourcen in Ihrem Amazon EKS-Cluster zugreifen können, AWS Resilience Hub muss die von verwendete IAM-Rolle einer Kubernetes-Gruppe mit ausreichenden Leseberechtigungen für Ressourcen in Ihrem Amazon EKS-Cluster zugeordnet sein.

AWS Resilience Hub ermöglicht den Zugriff auf Ihre Amazon EKS-Cluster-Ressourcen mithilfe einer der folgenden IAM-Rollenoptionen:

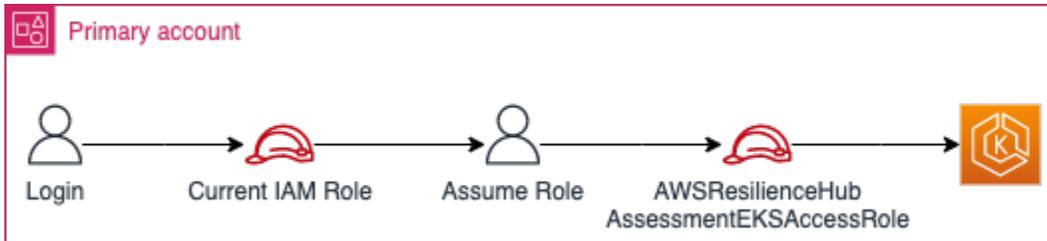
- Wenn Ihre Anwendung so konfiguriert ist, dass sie rollenbasierten Zugriff für den Zugriff auf Ressourcen verwendet, wird die Aufruferrolle oder sekundäre Kontorolle, an die Sie bei der Erstellung einer Anwendung übergeben wurden, AWS Resilience Hub während der Bewertung für den Zugriff auf Ihren Amazon EKS-Cluster verwendet.

Das folgende Konzeptdiagramm zeigt, wie AWS Resilience Hub auf Amazon EKS-Cluster zugegriffen wird, wenn die Anwendung als rollenbasierte Anwendung konfiguriert ist.

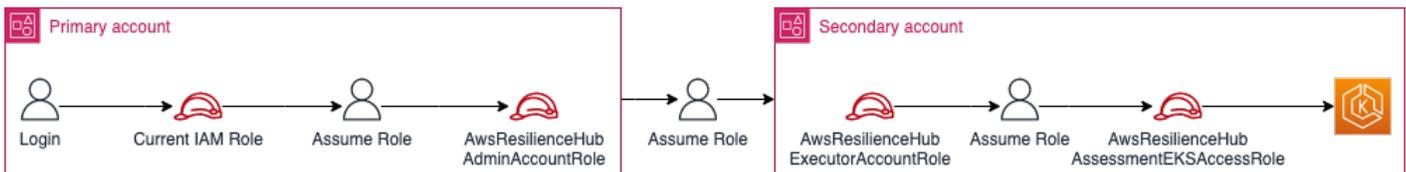


- Wenn Ihre Anwendung so konfiguriert ist, dass sie den aktuellen IAM-Benutzer für den Zugriff auf Ressourcen verwendet, müssen Sie eine neue IAM-Rolle mit dem Namen `AwsResilienceHubAssessmentEKSAccessRole` im gleichen Konto wie der des Amazon EKS-Clusters erstellen. Diese IAM-Rolle wird dann für den Zugriff auf Ihren Amazon EKS-Cluster verwendet.

Das folgende Konzeptdiagramm zeigt, wie auf Amazon EKS-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 Amazon EKS-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 Amazon EKS-Cluster gewähren

AWS Resilience Hub ermöglicht Ihnen den Zugriff auf Ressourcen, die sich auf Amazon EKS-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 Amazon EKS-Clusters zu erteilen

1. Konfigurieren Sie eine IAM-Rolle für den Zugriff auf den Amazon EKS-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 “So 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 Amazon EKS-Clusters erstellen. Diese IAM-Rolle wird dann beim Zugriff auf Ihren Amazon EKS-Cluster verwendet.

AWS Resilience Hub verwendet beim Import und der Bewertung Ihrer Anwendung eine IAM-Rolle, um auf die Ressourcen in Ihrem Amazon EKS-Cluster zuzugreifen. Diese Rolle sollte in demselben Konto wie Ihr Amazon EKS-Cluster erstellt werden. Sie wird einer Kubernetes-Gruppe zugeordnet, die die für die Bewertung Ihres Amazon EKS-Clusters erforderlichen Berechtigungen enthält. AWS Resilience Hub

Wenn sich Ihr Amazon EKS-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 die 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 Amazon EKS-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 den Amazon EKS-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` und gewährt `ClusterRoleBinding` die erforderlichen Leseberechtigungen für AWS Resilience Hub die Analyse und Bewertung von Ressourcen, die Teil bestimmter Namespaces in Ihrem Amazon EKS-Cluster sind.

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 auf alle Namespaces. AWS Resilience Hub

AWS Resilience Hub Um die Resilienz von Ressourcen in allen Namespaces innerhalb eines Amazon EKS-Clusters zu bewerten, müssen Sie das folgende und erstellen.

`ClusterRole` `ClusterRoleBinding`

- `resilience-hub-eks-access-cluster-role(ClusterRole)` — Definiert die Berechtigungen, die für AWS Resilience Hub die Bewertung Ihres Amazon EKS-Clusters erforderlich sind.
- `resilience-hub-eks-access-cluster-role-binding(ClusterRoleBinding)` — Definiert eine `resilience-hub-eks-access-group` in Ihrem Amazon EKS-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 für 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
  - replicaset
  verbs:
  - get
  - list
- apiGroups:
  - policy
  resources:
  - poddisruptionbudgets
verbs:
```

```
- get
- list
- apiGroups:
  - autoscaling.k8s.io
resources:
  - verticalpodautoscalers
verbs:
  - get
  - list
- apiGroups:
  - autoscaling
resources:
  - horizontalpodautoscalers
verbs:
  - get
  - list
- apiGroups:
  - karpenter.sh
resources:
  - provisioners
verbs:
  - get
  - list
- apiGroups:
  - karpenter.k8s.aws
resources:
  - awsnodeTemplates
verbs:
  - get
  - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
```

EOF

- b. 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 Amazon EKS-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 EKS-Cluster zu bewerten. AWS Resilience Hub erfordert Berechtigungen für den Zugriff auf Ressourcen im Clusterbereich (z. B. Knoten) in Ihrem Amazon EKS-Cluster, um die Ausfallsicherheit Ihrer Anwendung zu bewerten.

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
    verbs:
```

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

---
EOF
```

- **RoleBindingRolle** — 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 Amazon EKS-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
```

- **ClusterRoleBindingRolle** — 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 `resilience-hub-eks-access-group` IAM-Rolle zuzuordnen, die für den Zugriff auf den Amazon EKS-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 Amazon EKS-Clusters.

Note

- `ROLE-NAME` bezieht sich auf die IAM-Rolle, die für den Zugriff auf den Amazon EKS-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 der sein. `AwsResilienceHubAssessmentEKSAccessRole`
- `ACCOUNT-ID` sollte die AWS Konto-ID des Amazon EKS-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 sie manuell bearbeiten, `aws-auth ConfigMap` indem Sie die IAM-Rolldetails 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.

- ARN-Syntax —`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-Rolldetails zum `mapRoles` Abschnitt `ConfigMap` unter `Daten` 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 (Amazon SNS) -Themen aktivieren AWS Resilience Hub können. Um Push-Benachrichtigungen zu einem Amazon SNS SNS-Thema zu senden, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Eine aktive AWS Resilience Hub Anwendung.
- Ein vorhandenes Amazon SNS SNS-Thema, an das Benachrichtigungen gesendet AWS Resilience Hub werden müssen. Weitere Informationen zum Erstellen eines Amazon SNS SNS-Themas finden Sie unter [Erstellen eines Amazon SNS SNS-Themas](#).

Um Benachrichtigungen AWS Resilience Hub zu Ihrem Amazon SNS SNS-Thema veröffentlichen zu können, müssen Sie die Zugriffsrichtlinie für das Amazon SNS SNS-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 früher Nachrichten aus Regionen veröffentlichen, für die Sie sich angemeldet haben, zu Themen in Regionen, die standardmäßig aktiviert sind, müssen Sie die für das Amazon SNS SNS-Thema erstellte Ressourcenrichtlinie ändern. Ändern Sie den Wert von Principal von `resiliencehub.amazonaws.com` auf `resiliencehub.<opt-in-region>.amazonaws.com`

Wenn Sie ein Amazon SNS SNS-Thema mit serverseitiger Verschlüsselung (SSE) verwenden, müssen Sie sicherstellen, dass das Decrypt und GenerateDataKey * Zugriff auf den Amazon SNS SNS-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 für den Zugriff AWS Resilience Hub über das Netzwerk. Clients müssen Transport Layer Security (TLS) 1.2 oder höher unterstützen. Wir

empfehlen TLS 1.3 oder höher. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

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 [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 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 Support](#) Benutzerhandbuch.

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 tägliche Durchführung von Bewertungen in Ihrem Namen AWS Resilience Hub zu ermöglichen, führen Sie die Schritte unter So aktualisieren Sie die Resilienzabweichung Ihres Anwendungsverfahrens aus, indem Sie das Kontrollkästchen Diese Anwendung täglich automatisch bewerten aktivieren.)
- [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 Anwendungsbeurteilung — Prüft, wann Sie für jede Ihrer Anwendungen 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 unter Erkennung von AWS Resilience Hub Resilienzabweichungen das Kontrollkästchen Diese Anwendung täglich automatisch bewerten aktivieren. Um das Kontrollkästchen Diese Anwendung täglich automatisch bewerten zu aktivieren, füllen Sie das Verfahren So aktualisieren Sie die Erkennung von Stabilitätsabweichungen Ihrer Anwendung unter aus. [???](#)

Note

Bei dieser Prüfung wird das Bewertungsalter nur für die Anwendungen bestimmt, die mindestens einmal bewertet wurden. AWS Resilience Hub

- 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

- API-Version: aktuelle
- Letzte Aktualisierung der Dokumentation: 28. März 2024

Änderung	Beschreibung	Datum
AWS Trusted Advisor Verbesserungen	<p>AWS Resilience Hub hat die Unterstützung für erweitert, AWS Trusted Advisor indem eine Prüfung hinzugefügt wurde, um Anwendungskomponenten zu identifizieren, die nicht wiederhergestellt werden können ().</p> <p>AppComponents</p> <p>Weitere Informationen finden Sie unter the section called “AWS Trusted Advisor”.</p>	28. März 2024
AWS Resilience Hub erweitert die Unterstützung für empfohlene Alarme	<p>AWS Resilience Hub hat die README.md Vorlage mit Werten aktualisiert, mit denen Sie Alarme erstellen können, die von AWS Resilience Hub intern AWS (z. B. Amazon CloudWatch) oder extern empfohlen werden AWS.</p>	26. März 2024

Weitere Informationen finden Sie unter [the section called “Verwalten von Alarmen”](#).

[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 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.

26. März 2024

Weitere Informationen finden Sie unter den folgenden Themen:

- [the section called “Unterstützte AWS Resilience Hub Ressourcen”](#)
- [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#)

- [the section called “Gruppieren von Ressourcen in einem AppComponent”](#)

[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.

9. November 2023

Weitere Informationen finden Sie unter [the section called “Grundlegendes zu Resilienz werten”](#).

[AWS Resilience Hub erweitert die Unterstützung für Anwendungen, die Amazon Elastic Kubernetes Service \(Amazon EKS\) -Ressourcen enthalten](#)

AWS Resilience Hub erweitert die Unterstützung für Anwendungen, die Amazon EKS-Ressourcen enthalten, um neue Betriebsempfehlungen. Bei der Durchführung einer Bewertung, die Ressourcen aus Amazon EKS-Clustern einbezieht, empfehlen wir nun, Tests und Alarmer durchzuführen, um die Ausfallsicherheit der Anwendungen zu verbessern.

9. November 2023

Weitere Informationen finden Sie unter [the section called “Experimente mit dem Amazon Fault Injection Service”](#).

[AWS Resilience Hub bietet zusätzliche Informationen auf Anwendungsebene](#)

AWS Resilience Hub bietet zusätzliche Informationen auf Anwendungsebene über den geschätzten Workload-RTO und den geschätzten Workload-RPO. Diese zusätzlichen Informationen geben die maximal mögliche geschätzte Arbeitslast (RTO) und die geschätzte Arbeitslast (RPO) Ihrer Anwendung aus der letzten erfolgreichen Bewertung an. Bei diesem Wert handelt es sich um den geschätzten maximalen Workload-RTO und den geschätzten Workload-RPO für alle Störungstypen.

Weitere Informationen finden Sie unter [the section called “Anwendungen”](#).

30. Oktober 2023

[AWS Resilience Hub erweitert die Bewertungsunterstützung für Ressourcen AWS Step Functions](#)

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 Wiederherstellungszeitziele (RTO) und die geschätzten Wiederherstellungszeitziele (RPO) für Workloads 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 finden Sie unter [the section](#)

30. Oktober 2023

called “AWSResilienceHubAssessmentExecutionPolicy”.

[AWS Resilience Hub ermöglicht das Ausschließen von Betriebsempfehlungen](#)

9. August 2023

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 können Sie nun empfohlene Alarme, SOPs und AWS FIS Tests ausschließen, die für sie nicht relevant sind. 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”](#)

- [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 AWS Resilience Hub bietet. Es konsolidiert außerdem Berechtigungen in einer einzigen Rolle und bietet die Möglichkeit, benutzerdefinierte Rollennamen zu erstellen, 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 unter [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

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 (Amazon SNS), Benachrichtigungen zu erhalten, wenn das geschätzte Workload Recovery Time Objective (RTO) oder das geschätzte Workload Recovery Point Objective (RPO) nicht mehr das Ziel erreicht hat, sondern die Geschäftsziele Ihres Unternehmens nicht mehr erfüllt. Wenn Sie von der reaktiven Identifizierung von Problemen mit der Ausfallsicherheit bei der manuellen Durchführung einer Bewertung zur proaktiven Benachrichtigung über Amazon SNS SNS-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 die Erkennung von Stabilitätsabweichungen 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 RDS beinhalten, nun zwischen verschiedenen Datenbank-Engines unterscheiden, um genauere Schätzungen der Workload Recovery Time Objectives (RTOs) zu erhalten. AWS Resilience Hub bietet auch zusätzliche Maßnahmen zur Implementierung von Best Practices für Resilienz in Ihrer AWS Umgebung. Zu den Best Practices können Leistungseinblicke mit DevOps Guru für Amazon RDS, 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 unter [the section](#)

02. August 2023

[called “AWSResilienceHubAssessmentExecutionPolicy”](#).

[AWS Resilience Hub erweitert die Unterstützung für Amazon Elastic Block Store-Snapshots](#)

AWS Resilience Hub erweitert die Bewertungsunterstützung für Amazon Elastic Block Store (Amazon EBS), um Amazon EBS-Snapshots zu erkennen, die innerhalb derselben Amazon EBS-Region mithilfe direkter 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.

02. August 2023

Weitere Informationen finden Sie unter [Amazon Elastic Block Store \(Amazon EBS\)](#).

[Verbesserungen von Amazon Elastic Compute Cloud](#)

27. Juni 2023

AWS Resilience Hub hat die Unterstützung für Amazon Elastic Compute Cloud (Amazon EC2) erweitert. AWS ermöglicht seinen Kunden, die Amazon EC2 verwenden, die für ihre Anwendungsfälle geeignete Konfiguration für Anwendungen unterschiedlicher Größe auszuwählen. AWS Resilience Hub unterstützt die Bewertung der folgenden Amazon EC2 Konfigurationen:

- On-Demand-Instances.
- Instanzen werden von AWS Backup und nach gesichert AWS Elastic Disaster Recovery.
- Support für auto-scaling Gruppen mit Amazon Route 53 Application Recovery Controller (Route 53 ARC)

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"](#)

<u>AWS verwaltete Richtlinienaktualisierungen</u>	<u>Referenz zu Zugriffsberechtigungen</u> .	
	Es wurde eine neue Richtlinie hinzugefügt, die den Zugriff auf andere AWS Dienste für die Durchführung von Bewertungen ermöglicht.	26. Juni 2023
	Weitere Informationen finden Sie unter <u>the section called "AWSResilienceHubAssessmentExecutionPolicy"</u> .	
<u>Neue Amazon DynamoDB DynamoDB-Alarme für Betriebsempfehlungen</u>	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 <u>die AWS Identity and Access Management (IAM-) Richtlinie der Rolle aktualisieren</u> , die Sie verwenden.	2. Mai 2023
	Weitere Informationen finden Sie unter <u>the section called "AWS Resilience Hub Referenz zu Zugriffsberechtigungen"</u> .	

[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 Resilience 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 Widerstandsfähigkeit der Anwendung auswirken würden.

Weitere Informationen zur AWS Resilience Hub Altersprüfung 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 S3 CRR)/Amazon S3 Same-Region Replication (SRR), Versionierung und AWS Backup AWS Resilience Hub wird Amazon S3 nun im Hinblick auf die Konfiguration von Access Point für mehrere Regionen, Amazon S3 Replication Time Control (Amazon S3 RTC) und Backup Recovery (PITR) geprüft. AWS point-in-time

21. März 2023

Weitere Informationen finden Sie unter den folgenden Themen:

- [the section called “AWS Resilience Hub Referenz zu Zugriffsberechtigungen”](#)
- [Verwaltung Ihres Amazon S3 S3-Speichers](#)

[Zusätzliche Unterstützung für Amazon Elastic Kubernetes Service](#)

AWS Resilience Hub hat den Amazon EKS-Cluster als unterstützte Ressource für die Definition, Validierung und Nachverfolgung der Ausfallsicherheit von Anwendungen hinzugefügt. Kunden können Amazon EKS-Cluster zu neuen oder bestehenden Anwendungen hinzufügen und erhalten Bewertungen und Empfehlungen zur Verbesserung der Ausfallsicherheit. Kunden können mithilfe von Terraform, AWS CloudFormation, und Anwendungsressourcen hinzufügen. AWS Resource Groups AppRegistry. Darüber hinaus können Kunden einen oder mehrere Amazon EKS-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, sondern auch die allgemeine Ausfallsicherheit des Clusters analysieren.

21. März 2023

en. AWS Resilience Hub unterstützt statuslose Amazon EKS-Cluster-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 EKS-Cluster hinzu”](#)
- [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 (Amazon EFS) -Backup AWS Resilience Hub wird Amazon EFS nun auch für Amazon EFS-Replikation und AZ-Konfiguration geprüft.

21. März 2023

Weitere Informationen finden Sie unter den folgenden Themen:

- [the section called “Unterstützte AWS Resilience Hub Ressourcen”](#)
- [Was ist Amazon Elastic File System?](#)

[Support für Anwendungsingabequellen](#)

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.

21. Februar 2023

Weitere Informationen finden Sie unter [the section called “Anwendungsressourcen bearbeiten”](#).

[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.

21. Februar 2023

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”](#)

[Zusätzliche Unterstützung für Amazon Elastic Block Store](#)

Zusätzlich zur aktuellen Unterstützung von Amazon Elastic Block Store (Amazon EBS) -Volumes AWS Resilience Hub werden nun Amazon EBS-Snapshots anhand von Amazon Data Lifecycle Manager und Amazon EBS Fast Snapshot Restore (FSR) bewertet.

21. Februar 2023

Weitere Informationen finden Sie unter den folgenden Themen:

- [the section called “AWS Resilience Hub Referenz zu Zugriffsberechtigungen”](#)
- [Amazon Elastic Block Store \(Amazon EBS\)](#)

[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 Resilienzrichtlinie (RTO und RPO) erfüllt wurde oder nicht. Jedes Mal, wenn eine Bewertung ausgeführt 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.

18. November 2022

Weitere Informationen finden Sie unter [the section called “AWS Trusted Advisor”](#).

[Support für Amazon Simple Notification Service \(Amazon SNS\)](#)

AWS Resilience Hub bewertet jetzt Anwendungen, die Amazon SNS verwenden, indem die Amazon SNS SNS-Konfiguration, einschließlich der Abonnenten, analysiert wird, und gibt Empfehlungen zur Erfüllung der geschätzten Workload-Wiederherstellungsziele des Unternehmens (geschätzter Workload-RTO und geschätzter Workload-RPO) für die Anwendungen. Amazon SNS ist ein verwalteter Service, der Nachrichten von Verlagen (Produzenten) an Abonnenten (Verbraucher) übermittelt.

16. November 2022

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 einem AppComponent”](#)

[Zusätzliche Support für Amazon Route 53 Application Recovery Controller \(Amazon Route 53 ARC\)](#)

AWS Resilience Hub bewertet jetzt Amazon Route 53 ARC für Elastic Load Balancing und Amazon Relational Database Service (Amazon RDS). Dazu gehört auch die Beratung, wann Amazon Route 53 ARC von Vorteil wäre. Erweiterung AWS Resilience Hub der Unterstützung von Amazon Route 53 ARC Assessment 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 für Elastic Load Balancing und Amazon Relational Database Service (Amazon RDS). Dazu gehört auch die Beratung, wann Amazon Route 53 ARC von Vorteil wäre. Erweiterung AWS Resilience Hub der Unterstützung von Amazon Route 53 ARC Assessment 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 Anwendungskomponenten hinzugefügt](#)

Route53 und AWS Backup wurden der Liste der unterstützten Anwendungskomponenten-Ressourcen im AppComponent Gruppierungsbereich hinzugefügt.

01. Juli 2022

[Neuer Inhalt: Konzept zum Status der Anwendungskonformität](#)

Der Statustyp „Änderungen erkannt“ wurde hinzugefügt.

2. Juni 2022

[Wir stellen vor AWS Resilience Hub](#)

AWS Resilience Hub ist jetzt verfügbar. In diesem Leitfaden wird beschrieben, wie Sie AWS Resilience Hub Ihre Infrastruktur analysieren, Empfehlungen zur Verbesserung der Ausfallsicherheit Ihrer AWS Apps abrufen, Resilienzwerte 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.