aws

Entwicklerhandbuch

Amazon Application Recovery Controller (ARC)

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Application Recovery Controller (ARC): Entwicklerhandbuch

Copyright © 2025 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 ARC? 1
Vergleichen Sie Multi-AZ- und Multiregions-Funktionen 4
Multi-AZ-Wiederherstellung 6
Zonenverschiebung 6
Wie funktioniert eine Zonenverschiebung 7
AWS-Regionen 8
Komponenten der Zonenverschiebung 13
Daten- und Kontrollebenen 15
Preisgestaltung 16
Bewährte Methoden 16
API-Operationen 18
Beispiele für die Verwendung von CLI-Operationen 19
Unterstützte Ressourcen 24
Eine Zonenschicht starten, aktualisieren oder stornieren 36
Protokollierung und Überwachung 38
IAM für Zonenverschiebung 43
Zonaler Autoshift 55
Wie funktioniert Zonal Autoshift 57
Über Zonal Autoshift 65
AWS-Regionen 66
Zonale Autoshift-Komponenten 66
Daten- und Steuerungsebenen 70
Preisgestaltung 70
Bewährte Methoden 70
API-Operationen 75
Beispiele für die Verwendung von CLI-Operationen 76
Zonal Autoshift aktivieren und damit arbeiten 83
Testen von Zonal Autoshift mit AWS FIS 87
Protokollierung und Überwachung 88
Identitäts- und Zugriffsverwaltung 99
Wiederherstellung mehrerer Regionen 115
Routing-Steuerung 115
Über Routing-Steuerung 116
AWS Regionen 119

Komponenten 120
Daten- und Steuerungsebenen 123
Tagging 124
Preisgestaltung 125
Erste Schritte mit der Wiederherstellung in mehreren Regionen 125
Bewährte Methoden 127
API-Operationen 131
Beispiele für die Verwendung von CLI-Operationen 135
Arbeiten mit Routing-Steuerungskomponenten 152
Protokollierung und Überwachung 173
Identitäts- und Zugriffsverwaltung 177
Kontingente 193
Prüfung der Bereitschaft 194
Was ist eine Bereitschaftsprüfung? 195
AWS Regionen 203
Komponenten 204
Daten- und Kontrollebenen 206
Tagging 207
Preisgestaltung 208
Richten Sie eine robuste Anwendung ein 208
Bewährte Methoden 209
API-Operationen 210
Beispiele für die Verwendung von CLI-Operationen 213
Arbeiten mit Wiederherstellungsgruppen und Bereitschaftsprüfungen 223
Überwachung des Bereitschaftsstatus 229
Architekturempfehlungen einholen 231
Kontoübergreifende Autorisierungen erstellen 233
Bereitschaftsregeln, Ressourcentypen und ARNS 235
Protokollierung und Überwachung 256
Identitäts- und Zugriffsverwaltung 271
Kontingente 287
Codebeispiele 289
Grundlagen 289
Aktionen 290
Sicherheit 296
Datenschutz 297

Verschlüsselung im Ruhezustand 298
Verschlüsselung während der Übertragung 298
Identitäts- und Zugriffsverwaltung 298
Zielgruppe 298
Authentifizierung mit Identitäten 299
Verwalten des Zugriffs mit Richtlinien 303
So funktionieren die Funktionen von Amazon Application Recovery Controller (ARC) mit IAM 306
Beispiele für identitätsbasierte Richtlinien 306
AWS verwaltete Richtlinien 307
Fehlerbehebung 314
Protokollierung und Überwachung 316
Compliance-Validierung 317
Ausfallsicherheit 318
Sicherheit der Infrastruktur 319
Dokumentverlauf 320
..... cccxxxvi

Was ist ARC?

Amazon Application Recovery Controller (ARC) unterstützt Sie bei der Vorbereitung und Durchführung einer schnelleren Wiederherstellung von Anwendungen, die auf der AWS globalen Cloud-Infrastruktur ausgeführt werden.

ARC bietet die folgenden Funktionen:

- Wiederherstellung in mehreren AZ-Zonen (Multi-Availability Zone), einschließlich Zonal Shift und Zonal Autoshift, mit denen Sie sich nach Beeinträchtigungen einzelner AZ erholen können, indem Sie den Verkehr vorübergehend von einer beeinträchtigten AZ auf eine fehlerfreie AZ verlagern.
- Wiederherstellung in mehreren Regionen, einschließlich Routing-Steuerung für Failover und Bereitschaftsprüfung für die Anwendungsüberwachung.

Wiederherstellung in mehreren Verfügbarkeitszonen

Zonale Verschiebung

Sie können ARC Zonal Shift verwenden, um Störungen in einer einzelnen Availability Zone (AZ) schnell zu isolieren und diese zu beheben. Zonal Shift verlagert den Verkehr für eine unterstützte Ressource vorübergehend von einer beeinträchtigten AZ auf eine fehlerfreie Ressource AZs in derselben Region. AWS Wenn Sie eine Zonenverschiebung starten, kann sich Ihre Anwendung schnell erholen, z. B. nach der Bereitstellung von schlechtem Code durch einen Entwickler oder nach einer AWS Beeinträchtigung in einer einzelnen AZ. Durch die Verlagerung des Datenverkehrs weg von der beeinträchtigten AZ werden die Auswirkungen für Kunden reduziert, die Ihre Anwendung in der beeinträchtigten AZ verwenden.

Sie können eine Zonenverschiebung für jede unterstützte Ressource in Ihrem Konto in einer AWS Region starten. Zonenverschiebungen sind manuell und temporär. Wenn Sie eine zonale Schicht beginnen, müssen Sie einen (verlängerbaren) Ablauf von bis zu drei Tagen angeben. Informationen zur Aktivierung von Zonal Shift für unterstützte Ressourcen finden Sie unter. Unterstützte Ressourcen

Zonaler Autoshift

ARC Zonal Autoshift autorisiert AWS , den Verkehr in Ihrem Namen von einer beeinträchtigten AZ für unterstützte Ressourcen auf intakte Ressourcen in derselben Region umzuleiten. AZs AWS AWS startet einen zonalen Autoshift, wenn die interne Telemetrie anzeigt, dass in einer AZ in einer AWS Region eine Beeinträchtigung vorliegt, die sich möglicherweise auf Kunden auswirken könnte. Die

interne Telemetrie beinhaltet Metriken aus verschiedenen Quellen, darunter dem AWS Netzwerk und den Amazon- EC2 und Elastic Load Balancing Balancing-Diensten.

Zonale Autoshifts sind temporär. AWS beendet eine zonale automatische Verschiebung, wenn die internen Telemetrieanzeigen anzeigen, dass kein Problem oder potenzielles Problem mehr besteht.

Weitere Informationen zu diesen Funktionen finden Sie in den folgenden Kapiteln:

- Zonenverschiebung in ARC
- Zonaler Autoshift in ARC

Wiederherstellung in mehreren Regionen

Routing-Steuerung

Die äußerst zuverlässigen Routingkontrollen von ARC ermöglichen die Wiederherstellung mehrerer Regionen, sodass Ihre Anwendungen den DNS-Verkehr des Domain Name Systems über Regionen hinweg AWS per Failover abwickeln können.

Wenn Ihre Anwendung für den Betrieb von mehreren AWS Regionen aus konzipiert ist, können Sie die ARC-Routingsteuerung für ein Failover zwischen Regionen verwenden. Die Routingsteuerung ermöglicht es Ihnen, den Datenverkehr von einer beeinträchtigten AWS Region in eine fehlerfreie AWS Region umzuleiten, sodass Sie sicherstellen können, dass Ihre Anwendung weiterhin verfügbar ist. Die Routingsteuerung umfasst Sicherheitsregeln, die Sie vor unbeabsichtigten Folgen schützen, indem sie von Ihnen festgelegte Leitplanken vorschreiben. Sie können beispielsweise eine Sicherheitsregel festlegen, nach der nur eines Ihrer Anwendungsreplikate, ob aktiv oder im Standby-Modus, aktiviert und verwendet wird.

Prüfung der Einsatzbereitschaft

Die ARC-Bereitschaftsprüfung überwacht kontinuierlich AWS Ressourcenkontingente, Kapazität und Netzwerkrouting-Richtlinien und kann Sie über Änderungen informieren, die sich auf Ihre Fähigkeit auswirken könnten, ein Failover auf eine Replikatanwendung durchzuführen und eine Wiederherstellung nach einer Beeinträchtigung der Region durchzuführen. Kontinuierliche Bereitschaftsprüfungen stellen sicher, dass Sie Ihre regionsübergreifenden Anwendungen in einem für den Failover-Verkehr skalierten und konfigurierten Zustand beibehalten können.
Die Bereitschaftsprüfung ist bei der ersten Konfiguration von ARC und während des normalen Anwendungsbetriebs nützlich. Die Bereitschaftsüberprüfung ist nicht für den Einsatz im kritischen Pfad für ein Failover während eines Ereignisses vorgesehen.

Weitere Informationen zu diesen Funktionen finden Sie in den folgenden Kapiteln:

- Routing-Steuerung in ARC
- Bereitschaftsprüfung in ARC

Vergleichen Sie die Multi-AZ- und Multi-Region-Wiederherstellungsfunktionen in ARC

Zonal Shift, Zonal Autoshift und Routing-Steuerung in Amazon Application Recovery Controller (ARC) ermöglichen allesamt eine schnelle Wiederherstellung und helfen Ihnen, die Ausfallsicherheit Ihrer Anwendungen sicherzustellen. AWS Diese Funktionen sind hochverfügbar und unterstützen die Wiederherstellung in Szenarien, in denen Ihre Anwendung eine erhöhte Latenz oder eine verringerte Verfügbarkeit aufweist. Diese Funktionen helfen auch bei der schnellen Wiederherstellung von Anwendungen, indem sie den Datenverkehr von isolierten Beeinträchtigungen wegverlagern, wodurch die Auswirkungen und der Zeitverlust durch Beeinträchtigungen begrenzt werden.

Die Routing-Steuerung konzentriert sich in erster Linie auf AWS Anwendungen, die sich in mehreren AWS Regionen befinden (Multi-Region), während Zonal Shift und Zonal Autoshift bei Multi-AZ-Anwendungen nur die Verlagerung des Datenverkehrs für unterstützte Ressourcen unterstützen.

Die Informationen in der folgenden Tabelle enthalten einige der wichtigsten Funktionen von Zonal Shift, Zonal Autoshift und Routing Control. Anhand dieser Beschreibungen können Sie besser verstehen, warum eine bestimmte Option die beste Wahl für die Anforderungen der Anwendung sein könnte.

Routing-Steuerung	Zonenverschiebung	Zonaler Autoshift
Regional Leitet den Verkehr von einer AWS Region in eine andere um (hauptsächlich)	Zonal Leitet den Verkehr von einer Availability Zone weg Der Verkehr wird zu anderen Availability Zones in der Region geleitet, nicht zu einem bestimmten Ziel	Zonal Leitet den Verkehr von einer Availability Zone weg Der Verkehr wird zu anderen Availability Zones in der Region geleitet, nicht zu einem bestimmten Ziel
Erfordert eine Einrichtung Erfordert Konfiguration und Einrichtung	Möglicherweise ist eine Einrichtung erforderlich Für einige unterstützte Ressourcen ist eine Anmeldung erforderlich	Erfordert eine Einrichtung Muss für eine unterstützte Ressource aktiviert sein

Routing-Steuerung	Zonenverschiebung	Zonaler Autoshift
	Weitere Informationen finden Sie unter Unterstützte Ressourcen	Weitere Informationen finden Sie unter Unterstützte Ressourcen
Vom Kunden initiiert Der Kunde bestimmt, wann der Verkehr umgeleitet werden soll	Vom Kunden initiiert Der Kunde bestimmt, wann mit einer Zonenschicht begonnen werden soll	AWS-initiiert AWS verlagert den Anwendungsdatenverkehr in Ihrem Namen von einer AZ weg
Gebührenpflichtig Erfordert separate Gebühren für die Routing-Kontrolle	In den Dienstleistungen enthalten (ohne zusätzliche Kosten) Das Erstellen von Zonenverschiebungen, um den Verkehr weg zu lenken, AZs ist in den unterstützten Ressourcen enthalten	In den Services enthalten (ohne zusätzliche Kosten) Das Starten von Autoshifts, um den Verkehr in AZs Ihrem Namen wegzuleiten, ist in den unterstützten Ressourcen enthalten
Läuft nicht ab Der Datenverkehr kann auf unbestimmte Zeit auf ein Replikat umgeleitet werden	Temporär Alle Zonenschichten müssen so eingestellt sein, dass sie ablaufen	Vorübergehend AWS startet und beendet Autoshift

Weitere Informationen zu den einzelnen Funktionen finden Sie in den folgenden Kapiteln:

- Zonenverschiebung in ARC
- Zonaler Autoshift in ARC
- Routing-Steuerung in ARC

Verwenden Sie Zonal Shift und Zonal Autoshift, um Anwendungen in ARC wiederherzustellen

In diesem Abschnitt wird erklärt, wie Sie die Funktionen von Amazon Application Recovery Controller (ARC) nutzen können, um Ihre AWS Ressource nach einem Problem in einer beeinträchtigten Availability Zone (AZ) zuverlässig wiederherzustellen. Zonal Shift und Zonal Autoshift verlagern den Datenverkehr für eine unterstützte Ressource vorübergehend von einer beeinträchtigten AZ weg, wodurch die Zeit bis zur Wiederherstellung Ihrer Anwendungen reduziert wird.

Der Hauptunterschied zwischen Zonal Shift und Zonal Autoshift besteht darin, dass es sich bei der einen um eine manuelle Verkehrsverlagerung handelt, die Sie kontrollieren, und bei der anderen wird der Verkehr automatisch in Ihrem Namen von einer Beeinträchtigung weggeleitet.

- Mit Zonal Shift verlagern Sie den Verkehr für eine unterstützte Ressource manuell in eine Availability Zone und von AWS-Region dieser weg.
- Mit Zonal Autoshift wird der Datenverkehr für eine unterstützte Ressource automatisch von einer beeinträchtigten AZ wegverlagert und zu einer AZs fehlerfreien Ressource in derselben Region umgeleitet. AWS

In den folgenden Themen werden die Funktionen Zonal Shift und Zonal Autoshift sowie deren Verwendung beschrieben.

Themen

- Zonenverschiebung in ARC
- Zonaler Autoshift in ARC

Zonenverschiebung in ARC

Mit Amazon Application Recovery Controller (ARC) Zonal Shift können Sie den Datenverkehr für eine unterstützte Ressource von einer beeinträchtigten Availability Zone (AZ) in eine fehlerfreie AWS-Region Ressource AZs in derselben Region verlagern. Durch die Verlagerung des Datenverkehrs Ihrer Ressourcen von einer beeinträchtigten AZ werden Dauer und Schwere der Auswirkungen reduziert, die durch Stromausfälle oder Hardware- oder Softwareprobleme in einer AZ verursacht werden. Dies trägt dazu bei, Probleme zu minimieren und Ihre Anwendung schnell wiederherzustellen. Sie könnten sich dafür entscheiden, den Datenverkehr zu verlagern, z. B.

weil eine fehlerhafte Bereitstellung Latenzprobleme verursacht oder weil die Availability Zone beeinträchtigt ist.

Bei einigen AWS Ressourcen müssen Sie sich für die Verwendung von Zonal Shift anmelden, und einige Ressourcen werden automatisch aktiviert. Weitere Informationen finden Sie unter Unterstützte Ressourcen.

Bevor Sie mit einer Zonenverschiebung beginnen, müssen Sie Ihre Anwendung vorab skalieren und sicherstellen, dass Sie über ausreichend Kapazität verfügen, um den Datenverkehr von einer Availability Zone weg zu verlagern. Nach der Vorskalierung können Sie die Availability Zone auswählen, von der Sie wegwechseln möchten, und die Ressource, für die der Verkehr weggeleitet werden soll, und dann die Zonenverschiebung starten. Sie können die Schicht jederzeit abbrechen, sodass der Verkehr wieder zur ursprünglichen Availability Zone zurückkehrt. Weitere Informationen finden Sie unter Bewährte Methoden für zonale Schichten in ARC.

Bei allen Zonenverschiebungen handelt es sich um vorübergehende Abhilfemaßnahmen. Sie legen einen anfänglichen Ablauf fest, wenn Sie eine Zonenschicht beginnen, und zwar von einer Minute bis zu drei Tagen (72 Stunden). Sie können diesen Zeitraum verlängern, wenn Sie die Verkehrsverlagerung fortsetzen müssen.

In bestimmten Szenarien verlagert die Zonenverlagerung den Verkehr nicht von der AZ weg. Weitere Informationen finden Sie unter Unterstützte Ressourcen.

Wie funktioniert eine Zonenverschiebung

Wenn Sie eine zonale Schicht für eine unterstützte Ressource starten, wird der Verkehr für die Ressource aus der von Ihnen angegebenen Availability Zone (AZ) entfernt. Die von ARC unterstützten Ressourcen bieten Integrationen, die die angegebene AZ als fehlerhaft kennzeichnen, was dazu führt, dass der Verkehr von der beeinträchtigten AZ weg verlagert wird.

Der Verkehr beginnt sich zu verlagern — Wenn Sie in ARC eine Zonenverschiebung starten, werden Sie möglicherweise nicht sofort feststellen, dass der Verkehr die Availability Zone verlässt. Abhängig vom Verhalten des Clients und der Wiederverwendung von Verbindungen kann es eine kurze Zeit dauern, bis bestehende, laufende Verbindungen in der Availability Zone abgeschlossen sind. DNS-Einstellungen und andere Faktoren, einschließlich vorhandener Verbindungen, können in nur wenigen Minuten abgeschlossen werden, können jedoch länger dauern. Weitere Informationen finden Sie unter Sicherstellen, dass Verkehrsverlagerungen schnell abgeschlossen werden.

Ende der Verkehrsschicht — Wenn eine Zonenschicht abläuft oder Sie sie stornieren, ergreift ARC Maßnahmen, um die Verkehrsverlagerung zu beenden, und kehrt den Vorgang zum Starten einer

Verkehrsschicht um. Jetzt wird die wiederhergestellte AZ als für die Ressource verfügbar erkannt und der Verkehr fließt wieder zur AZ.

Sie müssen festlegen, dass alle zonalen Schichten ablaufen, wenn Sie die Schichten starten. Sie können zunächst festlegen, dass eine Zonenschicht in maximal drei Tagen (72 Stunden) abläuft. Sie können eine Zonenschicht jedoch jederzeit aktualisieren, um ein neues Ablaufdatum festzulegen. Sie können eine Zonenschicht auch vor ihrem Ablauf stornieren, wenn Sie bereit sind, den Verkehr in der Availability Zone wiederherzustellen.

Wenn der Verkehr nicht wegverlagert wird — In bestimmten Szenarien wird der Verkehr durch eine Zonenverschiebung nicht aus der Availability Zone verlagert. Nehmen wir zum Beispiel an, Sie starten eine Zonenverschiebung für einen Load Balancer, wenn die Load Balancer-Zielgruppen AZs keine Instances haben oder wenn alle Instances fehlerhaft sind. In diesem Szenario befindet sich der Load Balancer in einem Fail-Open-Status und der Start einer Zonenverschiebung verlagert den Traffic nicht.

Bevor Sie eine Zonenverschiebung für eine Ressource starten, stellen Sie sicher, dass alle Bedingungen für eine erfolgreiche Zonenverschiebung erfüllt sind. AWS Ressourcen gehen unterschiedlich mit Zonenverschiebungen um. Weitere Hinweise zur Unterstützung von Zonenverschiebungen finden Sie unter. Unterstützte Ressourcen

AWS-Region Verfügbarkeit für Zonal Shift

Detaillierte Informationen zu regionalen Support- und Service-Endpunkten für Amazon Application Recovery Controller (ARC) finden Sie unter Amazon Application Recovery Controller (ARC) - Endpunkte und Kontingente in der Amazon Web Services General Reference.

Zonal Shift und Zonal Autoshift sind derzeit in den hier aufgeführten Versionen verfügbar. AWS-Regionen Zonal Shift und Zonal Autoshift sind auch in den Regionen China verfügbar, d. h. in den Regionen China (Peking) und China (Ningxia). Bei Ressourcen, die Amazon Application Recovery Controller (ARC) verwenden, müssen möglicherweise zusätzliche Überlegungen angestellt werden. Weitere Informationen finden Sie unter Unterstützte Ressourcen.

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
USA Ost (Ohio)	us-east-2	arc-zonal-shift.us-east-2.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)
		arc-zonal-shift-fips.us-east-2.api.aws	HTTPS
		arc-zonal-shift.us-east-2.api.aws	HTTPS
USA Ost (Nord-Virginia)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-east-1.api.aws	HTTPS
		arc-zonal-shift.us-east-1.api.aws	HTTPS
USA West (Nordkalifornien)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-1.api.aws	HTTPS
		arc-zonal-shift.us-west-1.api.aws	HTTPS
USA West (Oregon)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-2.api.aws	HTTPS
		arc-zonal-shift.us-west-2.api.aws	HTTPS
Afrika (Kapstadt)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.af-south-1.api.aws	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-east-1.api.aws	HTTPS
Asien-Pazifik (Hyderabad)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-south-2.api.aws	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Jakarta)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com arc-zonal-shift.ap-southeast-3.api.aws	HTTPS HTTPS
Asien-Pazifik (Malaysia)	ap-southeast-5	arc-zonal-shift.ap-southeast-5.amazonaws.com arc-zonal-shift.ap-southeast-5.api.aws	HTTPS HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com arc-zonal-shift.ap-southeast-4.api.aws	HTTPS HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com arc-zonal-shift.ap-south-1.api.aws	HTTPS HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com arc-zonal-shift.ap-northeast-3.api.aws	HTTPS HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com arc-zonal-shift.ap-northeast-2.api.aws	HTTPS HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com arc-zonal-shift.ap-southeast-1.api.aws	HTTPS HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com arc-zonal-shift.ap-southeast-2.api.aws	HTTPS HTTPS

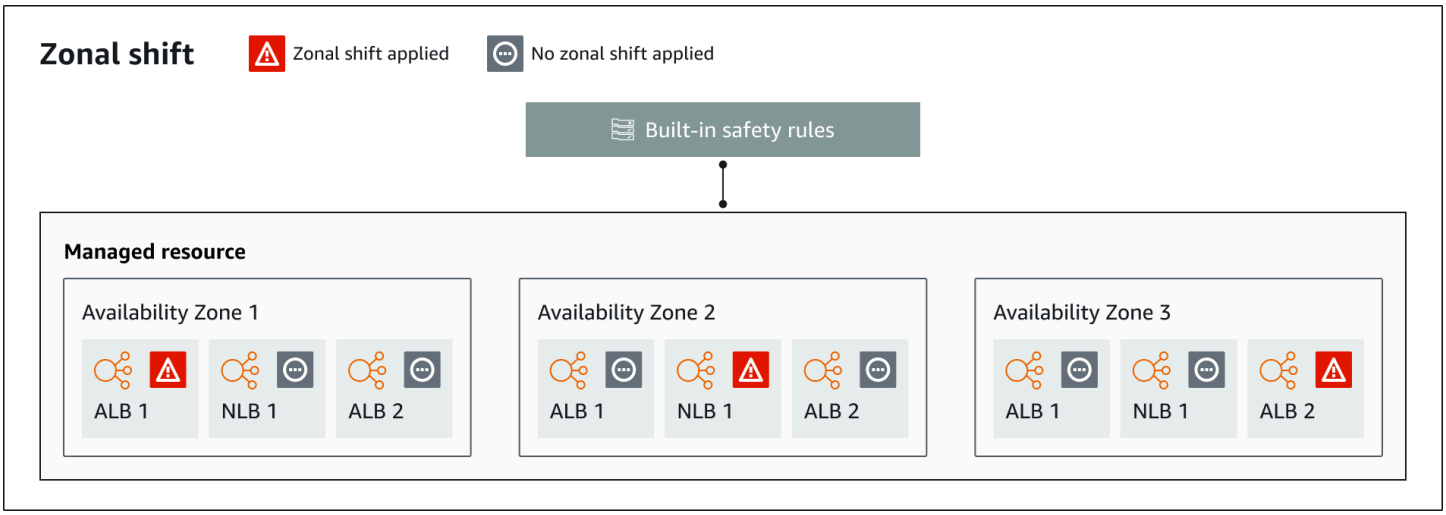
Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Thailand)	ap-southeast-7	arc-zonal-shift.ap-southeast-7.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-7.api.aws	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-northeast-1.api.aws	HTTPS
Kanada (Zentral)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-central-1.api.aws	HTTPS
		arc-zonal-shift.ca-central-1.api.aws	HTTPS
Kanada West (Calgary)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-west-1.api.aws	HTTPS
		arc-zonal-shift.ca-west-1.api.aws	HTTPS
Europa (Frankfurt)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-central-1.api.aws	HTTPS
Europa (Irland)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-1.api.aws	HTTPS
Europa (London)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-2.api.aws	HTTPS
Europa (Mailand)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-south-1.api.aws	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Paris)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com arc-zonal-shift.eu-west-3.api.aws	HTTPS HTTPS
Europa (Spanien)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com arc-zonal-shift.eu-south-2.api.aws	HTTPS HTTPS
Europa (Stockholm)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com arc-zonal-shift.eu-north-1.api.aws	HTTPS HTTPS
Europa (Zürich)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com arc-zonal-shift.eu-central-2.api.aws	HTTPS HTTPS
Israel (Tel Aviv)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com arc-zonal-shift.il-central-1.api.aws	HTTPS HTTPS
Mexiko (Zentral)	mx-central-1	arc-zonal-shift.mx-central-1.amazonaws.com arc-zonal-shift.mx-central-1.api.aws	HTTPS HTTPS
Naher Osten (Bahrain)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com arc-zonal-shift.me-south-1.api.aws	HTTPS HTTPS
Naher Osten (VAE)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com arc-zonal-shift.me-central-1.api.aws	HTTPS HTTPS
Südamerika (São Paulo)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com arc-zonal-shift.sa-east-1.api.aws	HTTPS HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
AWS GovCloud (US-Ost)	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-gov-east-1.api.aws	HTTPS
		arc-zonal-shift.us-gov-east-1.api.aws	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-gov-west-1.api.aws	HTTPS
		arc-zonal-shift.us-gov-west-1.api.aws	HTTPS

Komponenten der Zonenverschiebung

Das folgende Diagramm zeigt ein Beispiel für eine zonale Schicht, die den Verkehr von einer Availability Zone in eine verlagert. AWS-Region In die Zonenschicht integrierte Prüfungen verhindern, dass Sie eine weitere Zonenschicht für eine Ressource starten, für die bereits eine Schicht aktiv ist.



Im Folgenden sind die Komponenten der Zonal-Shift-Fähigkeit in ARC aufgeführt.

Zonenverschiebung

Sie starten eine Zonenverschiebung für eine verwaltete Ressource in Ihrem AWS Konto, um den Verkehr vorübergehend von einer Availability Zone in einer Region zu verlagern AWS-Region,

die AZs in der Region intakt ist, um sich schnell von einem Problem in einer AZ zu erholen. Weitere Informationen zu unterstützten Ressourcen für Zonal Shift finden Sie unter. Unterstützte Ressourcen

Integrierte Sicherheitschecks

In ARC integrierte Prüfungen verhindern, dass mehr als eine Verkehrsverlagerung für eine Ressource gleichzeitig wirksam ist. Das heißt, nur eine vom Kunden initiierte Zonenverschiebung, ein Übungslauf oder eine automatische Verschiebung für die Ressource kann den Verkehr aktiv von einer Availability Zone weg verlagern. Wenn Sie beispielsweise eine Zonenverschiebung für eine Ressource starten, obwohl diese derzeit mit Autoshift wegverlagert ist, hat Ihre Zonenverschiebung Vorrang. Weitere Informationen finden Sie unter Zonaler Autoshift in ARC und Ergebnisse von Übungsläufen.

Ressourcen-ID

Der Bezeichner für eine Ressource, die in eine zonale Schicht aufgenommen werden soll. Die Kennung ist der Amazon-Ressourcenname (ARN) für die Ressource.

Bei einer Zonenverschiebung können Sie in Ihrem Konto nur Ressourcen für einen AWS Service auswählen, der von ARC unterstützt wird. Weitere Informationen zu unterstützten Ressourcen für Zonal Shift finden Sie unter. Unterstützte Ressourcen

Verwaltete Ressource

Einige AWS Ressourcen müssen sich manuell für die Zonenverschiebung anmelden, andere werden automatisch aktiviert. Weitere Informationen zu den unterstützten Ressourcen für Zonal Shift finden Sie unter. Unterstützte Ressourcen

Ressourcenname

Der Name einer Ressource in ARC, die Sie für eine Zonenverschiebung angeben können.

Status (Status der zonalen Verschiebung)

Ein Status für eine zonale Schicht. Der `Status` für eine zonale Verschiebung kann einen der folgenden Werte haben:

- AKTIV: Die Zonenverschiebung ist gestartet und aktiv.
- ABGELAUFEN: Die Zonenschicht ist abgelaufen (die Ablaufzeit wurde überschritten).
- STORNIERT: Die Zonenschicht wurde storniert.

Status „Angewendet“

Der Status „Angewendet“ gibt an, ob für eine Ressource eine Schicht in Kraft ist. Die Schicht, die diesen Status hat, `APPLIED` bestimmt die Availability Zone, in die der Anwendungsdatenverkehr für eine Ressource verlagert wurde, und bestimmt, wann diese Schicht endet.

Art der Schicht

Definiert den zonalen Schichttyp. Der `shiftType` kann die folgenden Werte haben:

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- ÜBUNGSLAUF
- FIS_EXPERIMENT

Ablaufzeit (Ablaufzeit)

Die Ablaufzeit (Ablaufzeit) für eine Zonenschicht. Zonenverschiebungen sind temporär. Für eine Zonenschicht können Sie zunächst festlegen, dass eine Zonenschicht für bis zu drei Tage (72 Stunden) aktiv ist.

Wenn Sie eine Zonenschicht beginnen, geben Sie an, wie lange sie aktiv sein soll. Dieser ARC wird in eine Ablaufzeit (Ablaufzeit) umgerechnet. Sie können beispielsweise eine Zonenverschiebung stornieren, wenn Sie bereit sind, den Verkehr in der Availability Zone wiederherzustellen. Oder Sie können eine vom Kunden initiierte Zonenschicht verlängern, indem Sie sie aktualisieren und einen anderen Zeitraum angeben, in dem sie ablaufen soll.

Sie können Übungsläufe für zonale Schichten stornieren, die Teil von Zonal Autoshift sind.

Daten- und Steuerungsebenen für Zonal Shift

Denken Sie bei der Planung von Failover und Disaster Recovery darüber nach, wie robust Ihre Failover-Mechanismen sind. Es wird empfohlen, sicherzustellen, dass die Mechanismen, auf die Sie beim Failover angewiesen sind, hochverfügbar sind, sodass Sie sie bei Bedarf in einem Notfallszenario verwenden können. In der Regel sollten Sie, wann immer möglich, Datenebenenfunktionen für Ihre Mechanismen verwenden, um die größtmögliche Zuverlässigkeit und Fehlertoleranz zu gewährleisten. Vor diesem Hintergrund ist es wichtig zu verstehen, wie die Funktionalität eines Dienstes zwischen Steuerungsebenen und Datenebenen aufgeteilt ist und wann Sie sich darauf verlassen können, dass die Datenebene eines Dienstes extrem zuverlässig ist.

Wie bei den meisten AWS Diensten wird die Funktionalität für die Zonenverlagerung durch Steuerungsebenen und Datenebenen unterstützt. Beide sind zwar auf Zuverlässigkeit ausgelegt, eine Steuerungsebene ist jedoch für die Datenkonsistenz optimiert, während eine Datenebene für die Verfügbarkeit optimiert ist. Eine Datenebene ist auf Ausfallsicherheit ausgelegt, sodass sie die Verfügbarkeit auch bei Störungen aufrechterhalten kann, wenn eine Kontrollebene möglicherweise nicht verfügbar ist.

Im Allgemeinen ermöglicht Ihnen eine Kontrollebene grundlegende Verwaltungsfunktionen wie das Erstellen, Aktualisieren und Löschen von Ressourcen im Service. Eine Datenebene stellt die Kernfunktionalität eines Dienstes bereit.

Weitere Informationen zu Datenebenen, Kontrollebenen und dazu, wie Services AWS entwickelt werden, um Hochverfügbarkeitsziele zu erreichen, finden Sie im paper Statische Stabilität mithilfe von Availability Zones in der Amazon Builders' Library.

Preise für die Zonenverschiebung in ARC

Bei einer Zonenverschiebung können Sie eine Zonenverschiebung für unterstützte Ressourcen starten, um Ihre Anwendung nach einem Problem in einer Availability Zone wiederherzustellen. Für die Nutzung von Zonal Shift fallen keine zusätzlichen Gebühren an.

Detaillierte Preisinformationen für ARC und Preisbeispiele finden Sie unter ARC-Preise.

Bewährte Methoden für zonale Schichten in ARC

Wir empfehlen die folgenden bewährten Methoden für die Verwendung von Zonenschichten für die Multi-AZ-Wiederherstellung in ARC.

Topics

- Kapazitätsplanung und Vorskalierung
- Begrenzen Sie die Zeit, in der Clients mit Ihren Endpunkten verbunden bleiben
- Testen Sie den Beginn von Zonenschichten im Voraus
- Stellen Sie sicher, dass alle Availability Zones fehlerfrei sind und Traffic aufnehmen
- Verwenden Sie API-Operationen auf Datenebene für die Notfallwiederherstellung
- Verschieben Sie den Verkehr mit einer zonalen Verschiebung nur vorübergehend

Kapazitätsplanung und Vorskalierung

Stellen Sie sicher, dass Sie ausreichend Kapazität eingeplant und entweder vorab skaliert haben oder automatisch skalieren können, um die zusätzliche Belastung der Availability Zones zu bewältigen, wenn Sie eine Zonenschicht beginnen. Bei einer auf Wiederherstellung ausgerichteten Architektur wird in der Regel empfohlen, die Rechenkapazität vorab so zu skalieren, dass genügend Headroom vorhanden ist, um den Spitzenverkehr zu bewältigen, wenn eines Ihrer (normalerweise) drei Replikate offline ist.

Wenn Sie eine Zonenverschiebung für eine unterstützte Ressource starten und der Datenverkehr von einer AZ weg verlagert wird, wird die Kapazität, die Ihre Anwendung für Serviceanfragen verwendet hat, entfernt. Sie müssen sicherstellen, dass Sie eine Verlagerung des Datenverkehrs von einer AZ weg geplant haben und in den verbleibenden AZs Bereichen weiterhin Anfragen bearbeiten können.

Beschränken Sie die Zeit, in der Clients mit Ihren Endpunkten verbunden bleiben

Wenn Amazon Application Recovery Controller (ARC) den Datenverkehr von einer Beeinträchtigung wegleitet, beispielsweise mithilfe von Zonal Shift oder Zonal Autoshift, ist der Mechanismus, den ARC verwendet, um Ihren Anwendungsdatenverkehr zu verlagern, ein DNS-Update. Ein DNS-Update bewirkt, dass alle neuen Verbindungen vom beeinträchtigten Standort weggeleitet werden.

Clients mit bereits bestehenden offenen Verbindungen können jedoch weiterhin Anfragen an den beeinträchtigten Standort stellen, bis die Clients wieder eine Verbindung herstellen. Um eine schnelle Wiederherstellung zu gewährleisten, empfehlen wir, die Dauer zu begrenzen, für die Clients mit Ihren Endpunkten verbunden bleiben.

Testen Sie den Beginn von Zonenschichten im Voraus

Testen Sie regelmäßig, für Ihre Anwendung den Traffic von Availability Zones weg zu verlagern, indem Sie zonale Schichten starten. Planen Sie den Start von Zonenverschiebungen und führen Sie diese aus, vorzugsweise sowohl in Test- als auch in Produktionsumgebungen, als Teil regelmäßiger Failover-Tests zur Wiederherstellung Ihrer Anwendungen im Katastrophenfall. Regelmäßige Tests sind entscheidend, um sicherzustellen, dass Sie auf Probleme vorbereitet sind und das nötige Selbstvertrauen haben, um Probleme zu beheben, wenn ein Betriebsereignis eintritt.

Stellen Sie sicher, dass alle Availability Zones fehlerfrei sind und Traffic aufnehmen

Bei Zonenverschiebungen wird eine Ressource, d. h. ein Anwendungsreplikat, in einer Availability Zone als fehlerhaft markiert. Das bedeutet, dass Sie unbedingt sicherstellen müssen, dass die

Ressourcen in Ihren Anwendungen im Allgemeinen fehlerfrei sind und den Datenverkehr in den Availability Zones einer Region aktiv aufnehmen. Wir empfehlen, dass Sie Dashboards verwenden, um dies nachzuverfolgen, darunter beispielsweise Elastic Load Balancing Balancing-Metriken für fehlerhafte Ziele und BytesProcessed pro Availability Zone.

Erwägen Sie, den Zustand Ihrer Ressourcen von einer zweiten, angrenzenden Region aus zu überwachen. Der Vorteil dieses Ansatzes besteht darin, dass er die Erfahrung Ihrer Endbenutzer besser wiedergeben kann. Außerdem wird dadurch das Risiko verringert, dass sowohl Ihre Anwendung als auch Ihre Überwachung gleichzeitig von derselben Katastrophe betroffen sind.

Verwenden Sie API-Operationen auf Datenebene für die Notfallwiederherstellung

Um eine Zonenverschiebung zu starten, wenn Sie eine Anwendung schnell und mit wenigen Abhängigkeiten wiederherstellen müssen, empfehlen wir, die AWS Command Line Interface OR-API mit Aktionen zur zonalen Verschiebung zu verwenden, wenn möglich mit vorab gespeicherten Anmeldeinformationen. Aus Gründen der Benutzerfreundlichkeit können Sie Zonenverschiebungen auch in der AWS Management Console starten. Wenn jedoch eine schnelle, zuverlässige Wiederherstellung entscheidend ist, sind Operationen auf Datenebene die bessere Wahl. Weitere Informationen finden Sie im Referenzhandbuch zur Zonal Shift API.

Verschieben Sie den Verkehr mit einer Zonenverschiebung nur vorübergehend

Durch eine Zonenverlagerung wird der Verkehr vorübergehend von einer Availability Zone weg verlagert, um eine Beeinträchtigung zu minimieren. Sie sollten die Ressource für den Betrieb der Anwendung wiederherstellen, sobald Sie Maßnahmen zur Behebung eines Problems ergriffen haben. Dadurch wird sichergestellt, dass Ihre gesamte Anwendung wieder in ihren ursprünglichen, vollständig redundanten und belastbaren Zustand versetzt wird.

API-Operationen mit zonaler Verschiebung

In der folgenden Tabelle sind ARC-API-Operationen aufgeführt, die Sie mithilfe von Zonal Shift verwenden können, wodurch der Datenverkehr für Multi-AZ-Anwendungen von einer Availability Zone weggeleitet wird. Die Tabelle enthält auch Links zu relevanter Dokumentation.

Beispiele für die Verwendung gängiger Zonal Shift-API-Operationen mit dem finden Sie AWS Command Line Interface unterBeispiele für die Verwendung von AWS CLI mit Zonenverschiebung.

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Starten einer Zonenverschiebung	Siehe Starten einer Zonenschicht	Siehe StartZonalShift
Aktualisieren einer Zonenverschiebung	Siehe Aktualisierung oder Stornierung einer Zonenschicht	Siehe UpdateZonalShift
Zonenverschiebungen auflisten	Siehe Zonenverschiebung in ARC	Siehe ListZonalShifts
Listet verwaltete Ressourcen auf	Siehe Unterstützte Ressourcen	Siehe ListManagedResources
Holen Sie sich die verwaltete Ressource	Siehe Unterstützte Ressourcen	Siehe GetManagedResource
Abbrechen einer Zonenverschiebung	Siehe Aktualisierung oder Stornierung einer Zonenschicht	Siehe CancelZonalShift

Beispiele für die Verwendung von AWS CLI mit Zonenverschiebung

Dieser Abschnitt enthält Anwendungsbeispiele für die Verwendung von Zonal Shift und die Nutzung der AWS Command Line Interface Zonal Shift-Funktion in Amazon Application Recovery Controller (ARC) mithilfe von API-Operationen. Die Beispiele sollen Ihnen helfen, ein grundlegendes Verständnis für die Arbeit mit Zonal Shift mithilfe der CLI zu entwickeln.

Zonal Shift in ARC ermöglicht es Ihnen, den Datenverkehr für unterstützte Ressourcen vorübergehend von einer Availability Zone weg zu verlagern, sodass Ihre Anwendung weiterhin normal mit anderen Availability Zones in einer arbeiten kann. AWS-Region

Alle Zonenschichten sind temporär und müssen zunächst so eingestellt werden, dass sie innerhalb von drei Tagen ablaufen. Sie können eine zonale Schicht jedoch später aktualisieren, um ein neues Ablaufdatum festzulegen.

Weitere Informationen zur Verwendung von finden Sie in der AWS CLI Befehlsreferenz. AWS CLI Eine Liste der Zonal Shift-API-Aktionen und Links zu weiteren Informationen finden Sie unterAPI-Operationen mit zonaler Verschiebung.

Starten Sie Zonal Shift

Sie können eine Zonenverschiebung mit der CLI starten, indem Sie den `start-zonal-shift` Befehl verwenden.

```
aws arc-zonal-shift start-zonal-shift \
       --resource-identifier arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05 \
       --away-from use1-az1 \
       --expires-in 10m \
       --comment "Shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T21:37:26-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Holen Sie sich die verwaltete Ressource

Sie können Informationen zu einer verwalteten Ressource mit der CLI abrufen, indem Sie den `get-managed-resource` Befehl verwenden.

```
aws arc-zonal-shift get-managed-resource \
       --resource-identifier arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05
```

```
{
    "appliedWeights": {
        "use1-az1": 0.0,
        "use1-az2": 1.0,
```

```
        "use1-az6": 1.0
    },
    "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/app/
Testing/5a19403ecd42dc05",
    "autoshifts": [],
    "name": "Testing",
    "zonalAutoshiftStatus": "DISABLED",
    "zonalShifts": [
        {
            "appliedStatus": "APPLIED",
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
            "shiftType": "MANUAL"
        }
    ]
}
```

Verwaltete Ressourcen auflisten

Sie können die verwalteten Ressourcen in Ihrem Konto mit der CLI auflisten, indem Sie den `list-managed-resources` Befehl verwenden.

```
aws arc-zonal-shift list-managed-resources
```

```
{
    "items": [
        {
            "appliedWeights": {
                "use1-az1": 0.0,
                "use1-az2": 1.0,
                "use1-az6": 1.0
            },
            "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/
app/Testing/5a19403ecd42dc05",
            "autoshifts": [],
            "availabilityZones": [
                "use1-az1",
```

```
                "use1-az2",
                "use1-az6"
            ],
            "name": "Testing",
            "practiceRunStatus": "DISABLED",
            "zonalAutoshiftStatus": "DISABLED",
            "zonalShifts": [
                {
                    "appliedStatus": "APPLIED",
                    "awayFrom": "use1-az1",
                    "comment": "Shifting traffic away from use1-az1",
                    "expiryTime": "2024-12-17T21:37:26-08:00",
                    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
                    "startTime": "2024-12-17T21:27:26-08:00",
                    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
                }
            ]
        }
    ]
}
```

Zonenverschiebungen auflisten

Sie können die Zonenverschiebungen in Ihrem Konto mit der CLI auflisten, indem Sie den `list-zonal-shifts` Befehl verwenden.

```
aws arc-zonal-shift list-zonal-shifts
```

```
{
    "items": [
        {
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "status": "ACTIVE",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
        }
    ]
```

```
}
```

Zonenverschiebung aktualisieren

Sie können eine Zonenverschiebung mit der CLI aktualisieren, indem Sie den `update-zonal-shift` Befehl verwenden.

```
aws arc-zonal-shift update-zonal-shift \
       --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38 \
       --expires-in 1h \
       --comment "Still shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Zonenverschiebung abbrechen

Sie können eine Zonenverschiebung mit der CLI abbrechen, indem Sie den `cancel-zonal-shift` Befehl verwenden.

```
aws arc-zonal-shift cancel-zonal-shift \
       --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
```

```
}
```

Unterstützte Ressourcen

Amazon Application Recovery Controller (ARC) unterstützt derzeit die folgenden Ressourcen für Zonal Shift und Zonal Autoshift:

- Amazon EC2 Auto Scaling Scaling-Gruppen
- Amazon Elastic Kubernetes Service
- Application Load Balancermit aktiviertem oder deaktiviertem zonenübergreifendem Load Balancing
- Network Load Balancersmit aktiviertem oder deaktiviertem zonenübergreifendem Load Balancing

Spezifische Anforderungen für Network Load Balancer und Application Load Balancer finden Sie in den zusätzlichen Themen in diesem Abschnitt.

Informieren Sie sich über die folgenden Bedingungen für die Arbeit mit Zonal Shifts, Zonal Autoshift und Ressourcen in ARC:

- Eine Ressource muss aktiv und vollständig bereitgestellt sein, um den Verkehr auf sie verlagern zu können. Bevor Sie eine Zonenverschiebung für eine Ressource starten, stellen Sie sicher, dass es sich um eine verwaltete Ressource in ARC handelt. Sehen Sie sich beispielsweise die Liste der verwalteten Ressourcen in der an AWS Management Console, oder verwenden Sie den `get-managed-resource` Vorgang mit der ID der Ressource.
- Um eine zonale Schicht mit einer Ressource zu starten, muss diese in der Availability Zone bereitgestellt werden und AWS-Region dort, wo Sie die Schicht beginnen. Stellen Sie sicher, dass Sie eine Zonenverschiebung in derselben Region starten, in der sich die AZ befindet, von der Sie wegwechseln möchten, und dass sich die Ressource, für die Sie den Verkehr verlagern, ebenfalls in derselben AZ und Region befindet.
- Stellen Sie sicher, dass Sie über die richtigen IAM-Berechtigungen verfügen, um Zonal Shift mit einer Ressource zu verwenden. Weitere Informationen finden Sie unter IAM und Berechtigungen für Zonal Shift.
- Wenn sich ein Network Load Balancer oder Application Load Balancer im Status „Fail Open“ befindet, hat die Zonenverschiebung keine Auswirkung. Dieses Verhalten ist zu erwarten, da eine Zonenverschiebung nicht dazu führen kann, dass eine AZ fehlerhaft ist und dann der Verkehr AZs in eine andere Region verlagert wird, wenn der Load Balancer nicht geöffnet werden kann. Weitere

Informationen finden Sie unter Using Route 53 DNS Failover for your Load Balancer im Network Load Balancers User Guide und Using Route 53 DNS Failover for your Load Balancer user Guide.

- Wenn mehrere Load Balancer Traffic an dieselben Ziele weiterleiten, führt eine zonale Verschiebung auf einem zonenübergreifenden Load Balancer zu einer Verringerung der Zielkapazität für alle Load Balancer, auch wenn sie nicht zonal verschoben sind.

Amazon EC2 Auto Scaling Scaling-Gruppen

Eine Amazon EC2 Auto Scaling Scaling-Gruppe enthält eine Sammlung von EC2 Amazon-Instances, die für die Zwecke der automatischen Skalierung und Verwaltung als logische Gruppierung behandelt werden. Mit einer Auto Scaling Scaling-Gruppe können Sie auch Amazon EC2 Auto Scaling Scaling-Funktionen wie Ersatz für Integritätsprüfungen und Skalierungsrichtlinien verwenden. Sowohl die Beibehaltung der Anzahl der Instances in einer Auto Scaling-Gruppe als auch die Auto Scaling sind die Kernfunktionen des Amazon EC2 Auto Scaling-Service.

Zonal Shift für Auto Scaling Scaling-Gruppen verwenden

Verwenden Sie eine der folgenden Methoden, um Zonal Shift zu aktivieren.

Console

Um Zonal Shift in einer neuen Gruppe (Konsole) zu aktivieren

1. Folgen Sie den Anweisungen unter Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage erstellen und schließen Sie jeden Schritt des Verfahrens bis zu Schritt 10 ab.
2. Aktivieren Sie auf der Seite Mit anderen Diensten integrieren für ARC Zonal Shift das Kontrollkästchen, um Zonal Shift zu aktivieren.
3. Wählen Sie für Verhalten bei der Integritätsprüfung die Option Ungesund ignorieren oder Ungesund ersetzen aus. Wenn diese Option auf gesetzt ist`replace-unhealthy`, werden fehlerhafte Instances in der Availability Zone durch die aktive Zonenverschiebung ersetzt. Wenn diese Option auf gesetzt ist`ignore-unhealthy`, werden fehlerhafte Instances in der Availability Zone nicht durch die aktive Zonenschicht ersetzt.
4. Fahren Sie mit den Schritten unter Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage erstellen fort.

AWS CLI

Um die Zonenverschiebung für eine neue Gruppe zu aktivieren ()AWS CLI

Fügen Sie dem create-auto-scaling-group-Befehl den `--availability-zone-impairment-policy`-Parameter hinzu.

Der `--availability-zone-impairment-policy` Parameter hat zwei Optionen:

- ZonalShiftEnabled— Wenn auf gesetzt`true`, registriert Auto Scaling die Auto Scaling Scaling-Gruppe mit ARC-Zonenverschiebung, und Sie können eine Zonenverschiebung auf der ARC-Konsole starten, aktualisieren oder abbrechen. Wenn auf gesetzt`false`, hebt Auto Scaling die Auto Scaling Scaling-Gruppe von ARC Zonal Shift ab. Sie müssen Zonal Shift bereits aktiviert haben, um auf setzen zu können. `false`
- ImpairedZoneHealthCheckBehavior— Wenn diese Option auf gesetzt ist`replace-unhealthy`, werden fehlerhafte Instances in der Availability Zone durch die aktive Zonenschicht ersetzt. Wenn diese Option auf gesetzt ist`ignore-unhealthy`, werden fehlerhafte Instances in der Availability Zone nicht durch die aktive Zonenschicht ersetzt.

Das folgende Beispiel aktiviert die Zonenverschiebung für eine neue Auto Scaling Scaling-Gruppe mit dem Namen*my-asg*.

```
aws autoscaling create-auto-scaling-group \
  --launch-template LaunchTemplateName=my-launch-template,Version='1' \
  --auto-scaling-group-name my-asg \
  --min-size 1 \
  --max-size 10 \
  --desired-capacity 5 \
  --availability-zones us-east-1a us-east-1b us-east-1c \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Console

Um Zonal Shift für eine bestehende Gruppe (Konsole) zu aktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/und wählen Sie im Navigationsbereich Auto Scaling Groups aus.

2. Wählen Sie in der Navigationsleiste oben die AWS-Region aus, in der Sie Ihre Auto-Scaling-Gruppe erstellt haben.
3. Aktivieren Sie das Kontrollkästchen neben der Auto-Scaling-Gruppe.

   Im unteren Teil der Seite wird ein geteilter Bereich geöffnet.
4. Wählen Sie auf der Registerkarte Integrationen unter ARC Zonal Shift die Option Bearbeiten aus.
5. Markieren Sie das Kontrollkästchen, um Zonal Shift zu aktivieren.
6. Wählen Sie für Verhalten bei der Integritätsprüfung die Option Ungesund ignorieren oder Ungesund ersetzen aus. Wenn diese Option auf gesetzt ist`replace-unhealthy`, werden fehlerhafte Instances in der Availability Zone durch die aktive Zonenverschiebung ersetzt. Wenn diese Option auf gesetzt ist`ignore-unhealthy`, werden fehlerhafte Instances in der Availability Zone nicht durch die aktive Zonenschicht ersetzt.
7. Wählen Sie Aktualisieren.

AWS CLI

Um die Zonenverschiebung für eine bestehende Gruppe zu aktivieren ()AWS CLI

Fügen Sie dem update-auto-scaling-group-Befehl den `--availability-zone-impairment-policy`-Parameter hinzu.

Der `--availability-zone-impairment-policy` Parameter hat zwei Optionen:

- ZonalShiftEnabled— Wenn auf gesetzt`true`, registriert Auto Scaling die Auto Scaling Scaling-Gruppe mit ARC-Zonenverschiebung, und Sie können eine Zonenverschiebung auf der ARC-Konsole starten, aktualisieren oder abbrechen. Wenn auf gesetzt`false`, hebt Auto Scaling die Auto Scaling Scaling-Gruppe von ARC Zonal Shift ab. Sie müssen Zonal Shift bereits aktiviert haben, um auf setzen zu können. `false`
- ImpairedZoneHealthCheckBehavior— Wenn diese Option auf gesetzt ist`replace-unhealthy`, werden fehlerhafte Instances in der Availability Zone durch die aktive Zonenschicht ersetzt. Wenn diese Option auf gesetzt ist`ignore-unhealthy`, werden fehlerhafte Instances in der Availability Zone nicht durch die aktive Zonenschicht ersetzt.

Das folgende Beispiel aktiviert die Zonenverschiebung für die angegebene Auto Scaling Scaling-Gruppe.

```
aws autoscaling update-auto-scaling-group --auto-scaling-group-name my-asg \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Informationen zum Auslösen einer Zonenverschiebung finden Sie unter. Eine Zonenschicht starten, aktualisieren oder stornieren

So funktioniert Zonal Shift für Auto Scaling Scaling-Gruppen

Angenommen, Sie haben eine Auto Scaling Scaling-Gruppe mit den folgenden Availability Zones:

- `us-east-1a`
- `us-east-1b`
- `us-east-1c`

Sie stellen Fehler in der Zone fest `us-east-1a` und lösen eine Zonenverschiebung aus. Die folgenden Verhaltensweisen treten auf, wenn eine Zonenverschiebung ausgelöst wird. `us-east-1a`

- Skalierung — Auto Scaling startet alle neuen Kapazitätsanfragen in den fehlerfreien Availability Zones (`us-east-1b`und`us-east-1c`).
- Dynamische Skalierung — Auto Scaling verhindert, dass Skalierungsrichtlinien die gewünschte Kapazität verringern. Auto Scaling verhindert nicht, dass Skalierungsrichtlinien die gewünschte Kapazität erhöhen.
- Instanzaktualisierung — Auto Scaling verlängert das Timeout für jeden Instanzaktualisierungsprozess, der sich während einer aktiven Zonenverschiebung verzögert.

Auswahl des Verhaltens bei der Integritätsprüfung in der Availability Zone beeinträchtigt	Verhalten bei Gesundheitschecks
Ungesundes ersetzen	Instances, die als fehlerhaft erscheinen, werden in allen Availability Zones (`us-east-1a us-east-1b` , und`us-east-1c`) ersetzt.

Auswahl des Verhaltens bei der Integritätsprüfung in der Availability Zone beeinträchtigt	Verhalten bei Gesundheitschecks
Ungesunde Geräte ignorieren	Instanzen, die als fehlerhaft erscheinen, werden in `us-east-1b` und ersetzt. `us-east-1c` Instances in der Availability Zone werden nicht durch die aktive Zonenverschiebung () `us-east-1a` ersetzt.

Bewährte Methoden für die Verwendung von Zonal Shift

Um die hohe Verfügbarkeit Ihrer Anwendungen bei Verwendung von Zonal Shift aufrechtzuerhalten, empfehlen wir die folgenden bewährten Methoden.

- Überwachen EventBridge Sie Benachrichtigungen, um festzustellen, ob eine anhaltende Beeinträchtigung der Availability Zone vorliegt. Weitere Informationen finden Sie unter Automatisieren von Amazon EC2 Auto Scaling mit Event Bridge.
- Verwenden Sie Skalierungsrichtlinien mit entsprechenden Schwellenwerten, um sicherzustellen, dass Sie über genügend Kapazität verfügen, um den Verlust einer Availability Zone zu tolerieren.
- Legen Sie eine Richtlinie zur Instanzwartung fest, die mindestens einen fehlerfreien Prozentsatz von 100 vorsieht. Mit dieser Einstellung wartet Auto Scaling darauf, dass eine neue Instance einsatzbereit ist, bevor es eine fehlerhafte Instance beendet.

Für Kunden mit vorinstallierter Version empfehlen wir außerdem Folgendes:

- Wählen Sie bei der Integritätsprüfung für die Zone mit eingeschränkter Verfügbarkeit die Option Ungesunde Instanz ignorieren aus, da Sie die fehlerhafte Instanz während des Beeinträchtigungsereignisses nicht austauschen müssen.
- Verwenden Sie Zonal Autoshift in ARC für Ihre Auto Scaling Scaling-Gruppen. Die zonale Autoshift-Funktion Amazon Application Recovery Controller (ARC) ermöglicht es, den Verkehr für eine Ressource von einer Availability Zone weg von einer Availability Zone AWS zu verlagern, wenn eine Beeinträchtigung in einer AWS Availability Zone festgestellt wird. Weitere Informationen finden Sie unter Zonal Autoshift in ARC im Amazon Application Recovery Controller (ARC) Developer Guide.

Für Kunden mit zonenübergreifenden deaktivierten Load Balancern empfehlen wir außerdem:

- Verwenden Sie Balanced nur für die Verteilung in Ihrer Availability Zone.
- Wenn Sie Zonal Shift sowohl für Ihre Auto Scaling Scaling-Gruppe als auch für Ihre Load Balancer verwenden, stellen Sie sicher, dass Sie zuerst die Zonenverschiebung in Ihrer Auto Scaling Scaling-Gruppe stornieren. Warten Sie dann, bis die Kapazität auf alle Availability Zones verteilt ist, bevor Sie die Zonenverschiebung auf dem Load Balancer abbrechen.
- Aufgrund der Möglichkeit einer unausgewogenen Kapazität, wenn Sie Zonal Shift aktivieren und einen zonenübergreifenden deaktivierten Load Balancer verwenden, verfügt Auto Scaling über eine zusätzliche Validierung. Wenn Sie die bewährten Methoden befolgen, können Sie diese Möglichkeit bestätigen, indem Sie das Kontrollkästchen im Feld aktivieren AWS Management Console oder das `skip-zonal-shift-validation` Kennzeichen in`CreateAutoScalingGroup`,, oder verwenden. `UpdateAutoScalingGroup` `AttachTrafficSources`

Amazon Elastic Kubernetes Service

Amazon EKS bietet Funktionen, mit denen Sie Ihre Anwendungen widerstandsfähiger gegen Ereignisse wie den verschlechterten Zustand oder die Beeinträchtigung einer Availability Zone (AZ) machen können. Wenn Sie Ihre Workloads in einem Amazon EKS-Cluster ausführen, können Sie die Fehlertoleranz und Anwendungswiederherstellung Ihrer Anwendungsumgebung mithilfe von Zonal Shift oder Zonal Autoshift weiter verbessern.

Verwendung von Zonal Shift für Amazon Elastic Kubernetes Service

Verwenden Sie eine der folgenden Methoden, um Zonal Shift zu aktivieren. Weitere Informationen finden Sie unter Amazon EKS Zonal Shift aktivieren, um beeinträchtigte Availability Zones zu vermeiden.

Console

So aktivieren Sie Zonal Shift auf einem neuen Amazon EKS-Cluster (Konsole)

1. Suchen Sie den Namen und die Region des Amazon EKS-Clusters, den Sie bei ARC registrieren möchten.
2. Öffnen Sie die Amazon EKS-Konsole unter https://console.aws.amazon.com/eks/home#/clusters.
3. Wählen Sie Ihren Cluster aus.
4. Wählen Sie auf der Cluster-Informationsseite den Tab Overview aus.

5. Wählen Sie unter der Überschrift Zonal Shift die Schaltfläche Verwalten aus.
6. Wählen Sie „Aktivieren“ oder „Deaktivieren“ für EKS Zonal Shift.

AWS CLI

Um Zonal Shift auf einem neuen Amazon EKS-Cluster zu aktivieren ()AWS CLI

- Geben Sie den folgenden Befehl ein:

```
aws eks create-cluster --name my-eks-cluster --role-
arn my-role-arn-to-create-cluster --resources-vpc-config
 subnetIds=string,string,securityGroupIds=string,string,endpointPublicAccess=boolean,end
 --zonal-shift-config enabled=true
```

Um Zonal Shift auf einem vorhandenen Amazon EKS-Cluster zu aktivieren ()AWS CLI

- Geben Sie den folgenden Befehl ein:

```
aws eks update-cluster-config --name my-eks-cluster --zonal-shift-config
 enabled=true
```

Sie können eine Zonenverschiebung für einen Amazon EKS-Cluster auslösen, oder Sie können zulassen, dass dies für Sie AWS erledigt wird, indem Sie Zonal Autoshift aktivieren. Sobald Ihr Amazon EKS-Cluster Zonal Shift mit ARC aktiviert ist, können Sie mit der ARC-Konsole, der AWS CLI oder Zonal Shift und Zonal Autoshift eine Zonal Shift auslösen oder Zonal Autoshift aktivieren. APIs

Weitere Informationen zum Auslösen einer Zonenverschiebung finden Sie unter. Eine Zonenschicht starten, aktualisieren oder stornieren

Weitere Informationen zur Aktivierung von Amazon EKS mit Zonal Shift finden Sie im Thema Erfahren Sie mehr über ARC Zonal Shift in Amazon EKS im Amazon Elastic Kubernetes Service User Guide.

So funktioniert Zonal Shift für Amazon Elastic Kubernetes Service

Während einer Amazon EKS-Zonenverschiebung findet automatisch Folgendes statt:

- Alle Knoten in der betroffenen AZ werden gesperrt. Dadurch wird verhindert, dass der Kubernetes Scheduler neue Pods auf den Knoten in der fehlerhaften AZ plant.
- Wenn Sie Managed Node Groups verwenden, wird das Rebalancing der Availability Zone ausgesetzt und Ihre Auto Scaling Group (ASG) wird aktualisiert, um sicherzustellen, dass neue Amazon EKS Data Plane-Knoten nur im fehlerfreien Zustand gestartet werden. AZs
- Die Knoten in der fehlerhaften AZ werden nicht beendet und die Pods werden nicht aus diesen Knoten entfernt. Auf diese Weise soll sichergestellt werden, dass Ihr Datenverkehr nach Ablauf oder Ausfall einer Zonenschicht sicher an die AZ zurückgesendet werden kann, wo immer noch die volle Kapazität vorhanden ist.
- Der EndpointSlice Controller findet alle Pod-Endpunkte in der beeinträchtigten AZ und entfernt sie aus der entsprechenden Zone. EndpointSlices Dadurch wird sichergestellt, dass nur Pod-Endpunkte, die sich in einem fehlerfreien AZs Zustand befinden, gezielt Netzwerkverkehr empfangen. Wenn eine Zonenverschiebung storniert wird oder abläuft, aktualisiert der EndpointSlice Controller das so, dass die EndpointSlices Endpunkte in die wiederhergestellte AZ aufgenommen werden.

Weitere Informationen finden Sie im AWS Container-Blog.

Application Load Balancer

Verwendung von Zonal Shift für Application Load Balancers

Um Application Load Balancers mit Zonal Shift zu verwenden, müssen Sie die ARC-Zonal Shift-Integration in den Application Load Balancer Balancer-Attributen aktivieren. Application Load Balancer unterstützt Zonenverschiebung mit zonenübergreifenden aktivierten oder zonenübergreifenden deaktivierten Konfigurationen.

Bevor Sie die ARC-Integration aktivieren und mit der Nutzung von Zonal Shift beginnen, sollten Sie Folgendes überprüfen:

- Sie können eine Zonenverschiebung für einen bestimmten Load Balancer nur für eine Availability Zone starten. Eine Zonenverschiebung lässt sich nicht für mehrere Availability Zones starten.
- AWS entfernt proaktiv IP-Adressen von zonalen Load Balancer-Diensten aus DNS, wenn sich mehrere Infrastrukturprobleme auf Dienste auswirken. Prüfen Sie immer die aktuelle Kapazität der Availability Zone, bevor Sie mit einer Zonenverschiebung beginnen.
- Wenn ein Application Load Balancer das Ziel eines Network Load Balancers ist, starten Sie die Zonenverschiebung immer vom Network Load Balancer aus. Wenn Sie eine Zonenverschiebung

vom Application Load Balancer aus starten, erkennt der Network Load Balancer die Verschiebung nicht und sendet weiterhin Datenverkehr an den Application Load Balancer.

Sie können eine Zonenverschiebung für einen Load Balancer in der Elastic Load Balancing Balancing-Konsole (in den meisten Fällen AWS-Regionen) oder in der ARC-Konsole starten.

Console

Um Zonal Shift auf einem Load Balancer (Konsole) zu aktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsseite unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie den Namen des Application Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Stellen Sie unter Routing-Konfiguration der Availability Zone die ARC-Zonen-Shift-Integration auf Aktivieren ein.
6. Wählen Sie Speichern.

AWS CLI

Um Zonal Shift auf einem Load Balancer zu aktivieren ()AWS CLI

- Geben Sie den folgenden Befehl ein:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-alb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

Weitere Informationen zum Auslösen einer Zonenverschiebung finden Sie unter. Eine Zonenschicht starten, aktualisieren oder stornieren

Mit dieser `keepalive` Option können Sie konfigurieren, wie lange Verbindungen bestehen bleiben. Weitere Informationen finden Sie unter Dauer der Keepalive-Dauer des HTTP-Clients im Application Load Balancer Balancer-Benutzerhandbuch. Standardmäßig legen Application Load Balancer den Wert für die Keepalive-Dauer des HTTP-Clients auf 3600 Sekunden oder 1 Stunde fest. Wir empfehlen Ihnen, den Wert zu senken, um Ihrem Ziel für die Wiederherstellungszeit für Ihre Anwendung zu entsprechen, z. B. 300 Sekunden. Wenn Sie die Dauer einer HTTP-Client-

Keepalive-Dauer wählen, sollten Sie berücksichtigen, dass dieser Wert einen Kompromiss darstellt zwischen einer häufigeren Wiederherstellung der Verbindung im Allgemeinen, was sich auf die Latenz auswirken kann, und einer schnelleren Verlagerung aller Clients aus einer beeinträchtigten AZ oder Region.

So funktioniert Zonal Shift für Application Load Balancers

Wenn eine Zonenverschiebung auf einem Application Load Balancer mit aktiviertem zonenübergreifendem Load Balancing gestartet wird, wird der gesamte Datenverkehr zu Zielen in der betroffenen Availability Zone blockiert und die zonale IP-Adresse wird aus dem DNS entfernt.

Weitere Informationen finden Sie unter Integrationen für Ihren Application Load Balancer im Application Load Balancer Balancer-Benutzerhandbuch.

Network Load Balancers

Verwenden von Zonal Shift für Network Load Balancer

Um Network Load Balancers mit Zonal Shift zu verwenden, müssen Sie die ARC-Zonal Shift-Integration in den Network Load Balancer Balancer-Attributen aktivieren. Network Load Balancer unterstützt Zonenverschiebung mit zonenübergreifenden aktivierten oder zonenübergreifenden deaktivierten Konfigurationen.

Sie können wählen, für welche Ressourcen Sie sich für die Verwendung von Zonal Shift und Zonal Autoshift entscheiden und wann Sie ein Failaway in einer beeinträchtigten Availability Zone durchführen möchten. Sowohl mit dem Internet verbundene als auch interne Network Load Balancer werden unterstützt.

Um Zonal Shift für Ihren zonenübergreifenden Network Load Balancer zu aktivieren, müssen alle an den Load Balancer angeschlossenen Zielgruppen die folgenden Anforderungen erfüllen.

- Der zonenübergreifende Lastenausgleich muss aktiviert oder auf eingestellt sein. `use_load_balancer_configuration`
  - Weitere Informationen zum zielgruppenübergreifenden Lastenausgleich finden Sie unter Zonenübergreifender Lastenausgleich für Zielgruppen.
- Das Zielgruppenprotokoll muss TCP oder TLS sein.
  - Weitere Informationen zu den Zielgruppenprotokollen des Network Load Balancer finden Sie unter Routing-Konfiguration.

- Der Verbindungsabbruch für fehlerhafte Ziele muss deaktiviert werden.
  - Weitere Informationen zum Verbindungsabbruch bei Zielgruppen finden Sie unter Verbindungsabbruch für fehlerhafte Ziele.
- Die Zielgruppe darf keine Application Load Balancer als Ziele haben.
  - Weitere Informationen zu Application Load Balancers als Ziele finden Sie unter Verwenden von Application Load Balancers als Ziele eines Network Load Balancer.

Sie können eine Zonenverschiebung für einen Network Load Balancer starten, indem Sie das Widget AWS CLI, die AWS Konsole oder das Elastic Load Balancing Widget verwenden. Wenn ein Application Load Balancer das Ziel eines Network Load Balancers ist, müssen Sie die Zonenverschiebung vom Network Load Balancer aus starten. Wenn Sie die Zonenverschiebung vom Application Load Balancer aus starten, hört der Network Load Balancer nicht auf, Datenverkehr an den Application Load Balancer und seine Ziele zu senden.

Console

So aktivieren Sie Zonal Shift auf einem Load Balancer (Konsole)

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsseite unter Load Balancing die Option Load Balancers aus.
3. Wählen Sie den Namen des Network Load Balancer aus.
4. Klicken Sie auf der Registerkarte Attribute auf Bearbeiten.
5. Stellen Sie unter Routing-Konfiguration der Availability Zone die ARC-Zonen-Shift-Integration auf Aktivieren ein.
6. Wählen Sie Speichern.

AWS CLI

Um Zonal Shift auf einem Load Balancer zu aktivieren ()AWS CLI

- Geben Sie den folgenden Befehl ein:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-nlb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

Weitere Hinweise zum Auslösen einer Zonenverschiebung finden Sie unter. Eine Zonenschicht starten, aktualisieren oder stornieren

So funktioniert Zonal Shift für Network Load Balancer

ARC führt dazu, dass die Integritätsprüfung für den registrierten Network Load Balancer fehlschlägt, sodass der Network Load Balancer Balancer-Knoten in der beeinträchtigten AZ aus dem DNS entfernt wird, wenn Sie eine Zonenverschiebung auslösen. Der Network Load Balancer deaktiviert die Ziele in der betroffenen Zone, sodass sie keinen Traffic mehr empfangen. Elastic Load Balancing behandelt diese Ziele per Zonenverschiebung als deaktivierte Ziele. Ziele im deaktivierten Zustand erhalten weiterhin Zustandsprüfungen. Wenn die Ziele fehlerfrei sind und die Zonenverschiebung abläuft (oder abgebrochen) wird, wird das Routing zu Zielen in der zuvor beeinträchtigten Zone wieder aufgenommen.

Während der Zonenverschiebung auf Network Load Balancers mit aktiviertem zonenübergreifendem Load Balancing werden die IP-Adressen des zonalen Load Balancers aus DNS entfernt. Bestehende Verbindungen zu Zielen in der beeinträchtigten Availability Zone bleiben bestehen, bis sie organisch geschlossen werden, während neue Verbindungen nicht mehr an Ziele in der beeinträchtigten Availability Zone weitergeleitet werden.

Weitere Informationen finden Sie im Thema Zonal Shift for your Network Load Balancer im Network Load Balancer User Guide.

Eine Zonenschicht starten, aktualisieren oder stornieren

Dieser Abschnitt enthält Verfahren für die Arbeit mit Zonenschichten, einschließlich des Startens einer Zonenschicht und des Stornierens einer Zonenschicht.

Starten einer Zonenschicht

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine vom Kunden initiierte Zonenverschiebung auf der Amazon Application Recovery Controller (ARC) -Konsole starten. Informationen zum programmgesteuerten Arbeiten mit Zonal Shift finden Sie im Zonal Shift API-Referenzhandbuch.

Sie können nicht nur eine Zonenverschiebung in ARC starten, sondern auch eine Zonenverschiebung für einen Load Balancer in der Elastic Load Balancing Balancing-Konsole (in unterstützten Regionen) starten. Weitere Informationen finden Sie unter Zonal Shift im Elastic Load Balancing User Guide.

So starten Sie eine Zonenverschiebung

1. Öffnen Sie die ARC-Konsole unter. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. Wählen Sie unter Multi-AZ die Option Zonal Shift.
3. Wählen Sie auf der Seite Zonal Shift die Option Zonal Shift starten aus.
4. Wählen Sie die Availability Zone aus, von der Sie den Verkehr wegverlagern möchten.
5. Wählen Sie eine unterstützte Ressource aus der Ressourcentabelle aus, für die Sie den Verkehr wegverlagern möchten.
6. Wählen Sie unter Ablauf der Zonenschicht festlegen eine Ablaufzeit für die Zonenschicht aus, oder geben Sie sie ein. Eine Zonenschicht kann so eingestellt werden, dass sie anfänglich für 1 Minute oder bis zu drei Tage (72 Stunden) aktiv ist.

   Alle Zonenverschiebungen sind temporär. Sie müssen ein Ablaufdatum festlegen, aber Sie können aktive Schichten später aktualisieren, um einen neuen Ablaufzeitraum von bis zu drei Tagen festzulegen.
7. Geben Sie einen Kommentar ein. Sie können die Zonenverschiebung später aktualisieren, um den Kommentar zu bearbeiten, wenn Sie möchten.
8. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass durch den Start einer Zonenschicht die verfügbare Kapazität für Ihre Anwendung reduziert wird, da der Verkehr von der Availability Zone weg verlagert wird.
9. Wählen Sie Starten.

Aktualisierung oder Stornierung einer Zonenschicht

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Zonenverschiebung, die Sie initiieren, auf der Amazon Application Recovery Controller (ARC) -Konsole aktualisieren oder stornieren. Informationen zum programmgesteuerten Arbeiten mit Zonal Shift finden Sie im Zonal Shift API-Referenzhandbuch.

Sie können eine Zonenschicht aktualisieren, um ein neues Ablaufdatum festzulegen, oder den Kommentar für die Zonenschicht bearbeiten oder ersetzen. Sie können eine Zonenschicht jederzeit stornieren, bevor sie abläuft.

Sie können Zonenverschiebungen, die Sie initiiert haben, oder Zonenverschiebungen, die für eine Ressource AWS beginnen, für einen Übungslauf für zonale automatische Verschiebung stornieren.

Weitere Informationen zu Übungsschichten bei zonaler Autoshift finden Sie unter. So funktionieren zonale Autoshift- und Übungsläufe

So aktualisieren Sie eine zonale Schicht

1. Öffnen Sie die ARC-Konsole unter. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. Wählen Sie unter Multi-AZ die Option Zonal Shift.
3. Wählen Sie eine Zonenschicht aus, die Sie aktualisieren möchten, und wählen Sie dann Zonenschicht aktualisieren aus.
4. Wählen Sie für Ablauf der Zonenverschiebung festlegen optional ein Ablaufdatum aus oder geben Sie es ein.
5. Bearbeiten Sie unter Kommentar optional den vorhandenen Kommentar oder geben Sie einen neuen Kommentar ein.
6. Wählen Sie Aktualisieren.

Um eine Zonenschicht abzubrechen

1. Öffnen Sie die ARC-Konsole unter. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. Wählen Sie unter Multi-AZ die Option Zonal Shift.
3. Wählen Sie eine Zonenschicht aus, die Sie stornieren möchten, und wählen Sie dann Zonenschicht stornieren aus.
4. Wählen Sie im modalen Bestätigungsdialogfeld die Option Bestätigen.

Protokollierung und Überwachung von Zonenverschiebungen in Amazon Application Recovery Controller (ARC)

Sie können es AWS CloudTrail für die Überwachung der Zonenverschiebung in Amazon Application Recovery Controller (ARC) verwenden, um Muster zu analysieren und Probleme zu beheben.

Themen

- Protokollieren von Zonal Shift-API-Aufrufen mit AWS CloudTrail

Protokollieren von Zonal Shift-API-Aufrufen mit AWS CloudTrail

Zonal Shift for ARC ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ARC ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Zonal Shift als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der ARC-Konsole und Codeaufrufen an die ARC-API-Operationen für Zonal Shift.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Zonenverschiebungen. 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 CloudTrail, die an ARC für die Zonenverschiebung gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zur zonalen Schicht in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in ARC eine Aktivität für die Zonenverschiebung auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für die Zonenverschiebung in ARC, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail

- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle ARC-Aktionen werden vom Routing Control API Reference Guide für Amazon Application Recovery Controller protokolliert CloudTrail und sind im Routing Control API Reference Guide dokumentiert. Beispielsweise generieren Aufrufe der `StartZonalShift` und `ListManagedResources` -Aktionen Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

ARC-Ereignisse im Ereignisverlauf anzeigen

CloudTrail ermöglicht es Ihnen, aktuelle Ereignisse im Event-Verlauf einzusehen. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Grundlegendes zu Einträgen in der Zonenschichtprotokolldatei

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListManagedResources` Aktion für die Zonenverschiebung demonstriert.

```
{
```

```
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:14:41Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```


Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `StartZonalShift` Aktion mit einer Konfliktausnahme für Zonal Shift demonstriert.

```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:10:38Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "StartZonalShift",
     "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "errorCode": "ConflictException",
      "errorMessage": "There's already an active zonal shift for that resource
 identifier: 'arn:aws:testservice:us-west-2:077059137270:testResource/456apples'.
 Active zonal shift: 'bac23b74-176e-c073-de8f-484ca508910f'",
      "requestParameters": {
        "resourceIdentifier": "arn:aws:testservice:us-
west-2:077059137270:testResource/456apples",
        "awayFrom": "usw2-az1",
        "expiresIn": "2m",
        "comment": "HIDDEN_FOR_SECURITY_REASONS"
      },
      "responseElements": null,
      "requestID": "OP4OYXZ54HUPMIPGWH_EXAMPLE",
```

```
      "eventID": "0bca6660-e999-43a5-9008-EXAMPLE",
      "readOnly": false,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

Identity and Access Management für Zonenverschiebungen in Amazon Application Recovery Controller (ARC)

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um ARC-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Inhalt

- Wie funktioniert Zonal Shift mit IAM
- IAM und Berechtigungen für Zonal Shift
- Beispiele für identitätsbasierte Richtlinien für die Zonenverschiebung in ARC

Wie funktioniert Zonal Shift mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Zonal Shift in Amazon Application Recovery Controller (ARC) zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Zonal Shift verwendet werden können.

IAM-Funktionen, die Sie mit Zonal Shift verwenden können

IAM-Feature	Unterstützung für Zonal Shift
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja

IAM-Feature	Unterstützung für Zonal Shift
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für ARC

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 ARC-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien in Amazon Application Recovery Controller (ARC)

Ressourcenbasierte Richtlinien innerhalb von ARC

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.

Politische Maßnahmen zur Zonenverlagerung

Unterstützt Richtlinienaktionen: Ja

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

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 keinen passenden API-Vorgang 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 ARC-Aktionen für Zonal Shift finden Sie unter Actions defined by Amazon Route 53 Zonal Shift in der Service Authorization Reference.

Richtlinienaktionen in ARC für Zonal Shift verwenden vor der Aktion die folgenden Präfixe:

```
arc-zonal-shift
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Zum Beispiel das Folgende:

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift:action2"
         ]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "arc-zonal-shift:Describe*"
```

Beispiele für identitätsbasierte ARC-Richtlinien für Zonenverschiebungen finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Zonenverschiebung in ARC

Politische Ressourcen für die Zonenverlagerung

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 Ressourcentypen und ihrer Aktionen sowie der Aktionen ARNs, die Sie mit dem ARN jeder Ressource angeben können, finden Sie unter dem folgenden Thema in der Service Authorization Reference:

- Von Amazon Route 53 — Zonal Shift definierte Aktionen

Informationen zu den Aktionen und Ressourcen, die Sie mit einem Bedingungsschlüssel verwenden können, finden Sie unter dem folgenden Thema in der Service Authorization Reference:

- Von Amazon Route 53 — Zonal Shift definierte Bedingungsschlüssel

Beispiele für identitätsbasierte ARC-Richtlinien für Zonal Shift finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Zonenverschiebung in ARC

Schlüssel zu den Bedingungen der Richtlinien für die Zonenverlagerung

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 Zustandstasten für zonale Umschaltungen finden Sie unter dem folgenden Thema in der Service Authorization Reference:

- Von Amazon Route 53 — Zonal Shift definierte Bedingungsschlüssel

Informationen zu den Aktionen und Ressourcen, die Sie mit einem Bedingungsschlüssel verwenden können, finden Sie in den folgenden Themen in der Service Authorization Reference:

- Von Amazon Route 53 — Zonal Shift definierte Aktionen

- Von Amazon Route 53 — Zonal Shift definierte Ressourcentypen

Beispiele für identitätsbasierte ARC-Richtlinien für Zonal Shift finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Zonenverschiebung in ARC

Zugriffskontrolllisten () in ARC ACLs

Unterstützt ACLs: Nein

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

Attributbasierte Zugriffskontrolle (ABAC) mit ARC

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt 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 Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

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

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

ARC bietet die folgende teilweise Unterstützung für ABAC:

- Zonal Shift unterstützt ABAC für verwaltete Ressourcen, die in ARC für Zonal Shift registriert sind. Weitere Informationen zu den verwalteten Ressourcen von ABAC for Network Load Balancer und Application Load Balancer finden Sie unter ABAC with Elastic Load Balancing im Elastic Load Balancing User Guide.

Temporäre Anmeldeinformationen mit ARC verwenden

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 von einer Benutzerrolle zu einer IAM-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.

Serviceübergreifende Prinzipalberechtigungen für ARC

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie eine IAM-Entität (Benutzer oder Rolle) verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Richtlinien erteilen einem Prinzipal-Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen.

Informationen darüber, ob für eine Aktion zusätzliche abhängige Aktionen in einer Richtlinie erforderlich sind, finden Sie unter dem folgenden Thema in der Service Authorization Reference:

- Amazon Route 53 Zonenverschiebung

Servicerollen für ARC

Unterstützt Servicerollen: Nein

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.

Dienstbezogene Rollen für ARC

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte 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. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Zonal Shift verwendet keine dienstbezogenen Rollen.

IAM und Berechtigungen für Zonal Shift

Dieser Abschnitt enthält zusätzliche Informationen darüber, wie Berechtigungen für die Zonal Shift-Funktion in Amazon Application Recovery Controller (ARC) funktionieren, insbesondere wenn Sie mit der Funktion von einem anderen AWS Service wie Elastic Load Balancing arbeiten. Informationen zur Funktionsweise von ARC-Funktionen mit IAM und zu Berechtigungen im Allgemeinen finden Sie in den Informationen im Übersichtsthema. Identity and Access Management für Zonenverschiebungen in Amazon Application Recovery Controller (ARC)

Zonal Shift unterstützt Application Load Balancers, Network Load Balancers, Amazon EC2 Auto Scaling Scaling-Gruppen und Amazon EKS. Sie können IAM-Bedingungsschlüssel verwenden, um eine IAM-Berechtigungsrichtlinie auf diese Ressourcen auszudehnen. Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die einen Bedingungsschlüssel mit mehreren Ressourcen unterschiedlichen Typs verwendet:

```
{
    "Condition": {
        "StringLike": {
```

```
            "arc-zonal-shift:ResourceIdentifier": [
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/
*",
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/
*",
                "arn:aws:eks:us-east-1:123456789012:cluster/*"
            ]
        }
    },
    "Action": [
        "arc-zonal-shift:StartZonalShift"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
```

Weitere Informationen finden Sie unter Unterstützte Ressourcen.

Zusätzlich zu den im IAM-Übersichtsthema beschriebenen Berechtigungen gilt Folgendes für die Zonenverschiebung für IAM und für Berechtigungen:

- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen für die Arbeit mit Zonal Shift in ARC verfügen. Weitere Informationen finden Sie unter Zugriff auf die Zonal Shift Console und Access Zonal Shift Operations.
- Sie müssen keine zusätzlichen Elastic Load Balancing Balancing-Berechtigungen mit IAM hinzufügen, um mit Zonenverschiebungen für verwaltete Load Balancer-Ressourcen in Ihrem Konto in ARC zu arbeiten.
- Eine AWS verwaltete Richtlinie, die vollen Zugriff für Elastic Load Balancing bietet, beinhaltet Berechtigungen für die Arbeit mit zonalen Schichten. Wenn Sie AWS verwaltete Richtlinien für den Zugriff auf Elastic Load Balancing verwenden, benötigen Sie keine zusätzlichen Berechtigungen in IAM for Zonal Shift, um Zonal Shifts für Load Balancer zu starten oder in der Elastic Load Balancing Balancing-Konsole damit zu arbeiten. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Elastic Load Balancing.

Beispiele für identitätsbasierte Richtlinien für die Zonenverschiebung in ARC

Standardmäßig sind Benutzer und Rollen nicht berechtigt, ARC-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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von ARC definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Application Recovery Controller (ARC) in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Beispiel: Zugriff auf die Konsole mit Zonal Shift
- Beispiel: Zonal Shift-API-Aktionen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand ARC-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 Richtlinienvalidierung mit 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 Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Beispiel: Zugriff auf die Konsole mit Zonal Shift

Um auf die Amazon Application Recovery Controller (ARC) -Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den ARC-Ressourcen in Ihrem aufzulisten und anzuzeigen 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 API 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 Benutzern vollen Zugriff auf die Nutzung von Zonal Shift in zu gewähren AWS Management Console, fügen Sie dem Benutzer eine Richtlinie wie die folgende hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

Beispiel: Zonal Shift-API-Aktionen

Die Zonal Shift-API leitet den Datenverkehr vorübergehend von einer Availability Zone weg, um eine Anwendung wiederherzustellen.

Um sicherzustellen, dass ein Benutzer Zonal Shift-API-Aktionen verwenden kann, fügen Sie eine Richtlinie hinzu, die den API-Vorgängen entspricht, mit denen der Benutzer arbeiten muss, z. B. die folgenden:

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

```
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        }
    ]
}
```

Zonaler Autoshift in ARC

Mit Zonal Autoshift autorisieren AWS Sie, den Ressourcenverkehr für eine Anwendung bei Ereignissen in Ihrem Namen aus einer Availability Zone (AZ) zu verlagern, um die Zeit bis zur Wiederherstellung zu verkürzen. AWS startet eine automatische Verschiebung, wenn die interne Telemetrie anzeigt, dass eine Beeinträchtigung der Availability Zone vorliegt, die sich möglicherweise auf Kunden auswirken könnte. Wenn Autoshift AWS gestartet wird, verlagert sich der Anwendungsdatenverkehr zu Ressourcen, die Sie für zonales Autoshift konfiguriert haben, von der Availability Zone weg.

Beachten Sie, dass ARC den Zustand einzelner Ressourcen nicht überprüft. AWS startet einen Autoshift, wenn AWS Telemetrie feststellt, dass eine Beeinträchtigung der Availability Zone vorliegt, die sich möglicherweise auf Kunden auswirken könnte. In einigen Fällen kann der Verkehr zu Ressourcen verlagert werden, die nicht beeinträchtigt werden.

Mit Zonal Autoshift autorisieren Sie auch, AWS den Ressourcenverkehr für eine Anwendung in Ihrem Namen aus einer Availability Zone für regelmäßige Übungsläufe zu verlagern. Für zonales Autoshift sind Übungsläufe erforderlich. Mithilfe der Zonenverschiebungen, die ARC für Übungsläufe startet, können Sie sicherstellen, dass die Verlagerung des Datenverkehrs aus einer Availability Zone während eines Autoshifts für Ihre Anwendung sicher ist. In regelmäßigen Übungsläufen wird getestet, ob Ihre Anwendung ohne eine Availability Zone normal funktionieren kann, indem zonale Verschiebungen gestartet werden, die den Verkehr für eine Ressource von einer Availability Zone weg verlagern. Übungsläufe finden wöchentlich statt und liefern ein Ergebnis (z. B. `SUCCEEDED` oder), anhand dessen Sie feststellen können`FAILED`, ob die Anwendung wie erwartet funktioniert.

> **Important**
>
> Bevor Sie Übungsläufe konfigurieren oder Zonal Autoshift aktivieren, empfehlen wir dringend, die Kapazität Ihrer Anwendungsressourcen in allen Availability Zones in der Region, in der Ihre Anwendungsressourcen bereitgestellt werden, vorab zu skalieren. Wenn ein Autoshift- oder Übungslauf gestartet wird, sollten Sie sich nicht auf die bedarfsorientierte Skalierung verlassen. Zonal Autoshift, einschließlich Übungsläufen, funktioniert unabhängig und wartet nicht, bis die Auto Scaling-Aktionen abgeschlossen sind. Wenn Sie sich auf Auto Scaling statt auf Vorskalierung verlassen, kann es länger dauern, bis Ihre Anwendung wiederhergestellt ist.
>
> Wenn Sie Auto Scaling verwenden, um regelmäßige Verkehrszyklen zu bewältigen, empfehlen wir Ihnen dringend, die Mindestkapazität Ihres Auto Scaling so zu konfigurieren, dass es auch beim Verlust einer Availability Zone normal weiterläuft.

Wenn Sie planen, zonales Autoshift zu aktivieren oder Übungsläufe zu konfigurieren, testen Sie, nachdem Sie die Kapazität Ihrer Anwendungsressourcen vorab skaliert haben, ob Ihre Anwendung auch ohne eine Availability Zone normal funktionieren kann. Um dies zu testen, starten Sie eine zonale Verschiebung, um den Verkehr für eine Ressource von einer Availability Zone weg zu verlagern.

Um sicherzustellen, dass Ihre Tests mit Zonal Shift effektiv sind, müssen Sie überprüfen, ob der Traffic von der AZ, von der Sie wegwechseln, erwartungsgemäß abfließt. Beispielsweise bieten sowohl Application Load Balancers als auch Network Load Balancers in Amazon Metriken pro AZ, mit CloudWatch denen Sie dies überwachen können. Je nachdem, wie lange ein Service und die Clients Verbindungen wiederverwenden, kann der Datenverkehr zu der AZ, von der Sie sich entfernt haben, länger als erwartet fortgesetzt werden. Weitere Informationen finden Sie unter Beschränken Sie die Zeit, in der Kunden mit Ihren Endpunkten verbunden bleiben.

Nachdem Sie durch den Start und die Auswertung einer Zonenverschiebung überprüft haben, ob Ihre Anwendung auch dann normal weiterlaufen kann, wenn der Datenverkehr von einer Availability Zone weg verlagert wird, können Sie anhand der regelmäßigen Übungsläufe, die ARC durchführt, kontinuierlich überprüfen, ob Sie über genügend Kapazität für eine automatische Verschiebung verfügen.

Zusätzlich zur Aktivierung von Zonal Autoshift für eine unterstützte Ressource in der ARC-Konsole haben Sie die Möglichkeit, stattdessen Zonal Autoshift für einen bestimmten Load Balancer in der

Amazon-Konsole zu aktivieren. EC2 Weitere Informationen zur Aktivierung von Zonal Autoshift mit Elastic Load Balancing finden Sie unter Zonal Shift im Elastic Load Balancing User Guide.

Autoshifts und Practice Run Zonal Shifts sind temporär. Bei Autoshifts wird bei Wiederherstellung der betroffenen Availability Zone die Verlagerung des Datenverkehrs für Ressourcen aus der Availability Zone AWS beendet. Der Anwendungsdatenverkehr für Kunden kehrt zu allen Availability Zones in der Region zurück. Bei einem Testlauf wird der Datenverkehr für eine einzelne Ressource für etwa 30 Minuten von einer Availability Zone weg verlagert und dann zurück zu allen Availability Zones in der Region verlagert.

Sie können EventBridge Amazon-Benachrichtigungen so konfigurieren, dass Sie über automatische Verschiebungen und Übungsläufe informiert werden. Weitere Informationen finden Sie unter Zonal Autoshift mit Amazon verwenden EventBridge.

So funktionieren zonale Autoshift- und Übungsläufe

Die zonale Autoshift-Funktion in Amazon Application Recovery Controller (ARC) ermöglicht es, den Verkehr für eine Ressource in Ihrem Namen von einer Availability Zone weg AWS zu verlagern, wenn AWS festgestellt wird, dass eine Beeinträchtigung vorliegt, die sich möglicherweise auf Kunden in der Availability Zone auswirken könnte. Zonal Autoshift ist für eine Ressource konzipiert, die in allen Availability Zones in einer vorskaliert ist AWS-Region, sodass eine Anwendung auch nach dem Verlust einer Availability Zone normal ausgeführt werden kann.

Bei Zonal Autoshift müssen Sie Übungsläufe konfigurieren, bei denen ARC den Datenverkehr für die Ressource regelmäßig von einer Availability Zone weg verlagert. ARC plant etwa wöchentlich Übungsläufe für jede Ressource, der eine Übungslaufkonfiguration zugeordnet ist. Übungsläufe für jede Ressource werden unabhängig voneinander geplant.

Für jeden Übungslauf zeichnet ARC ein Ergebnis auf. Wenn ein Übungslauf durch eine Blockierung unterbrochen wird, wird das Ergebnis des Übungslaufs nicht als erfolgreich markiert. Weitere Informationen zu den Ergebnissen von Übungsläufen finden Sie unter Ergebnisse von Übungsläufen.

Sie können EventBridge Amazon-Benachrichtigungen so konfigurieren, dass Sie Informationen zu Autoshifts und Übungsläufen erhalten. Weitere Informationen finden Sie unter Zonal Autoshift mit Amazon verwenden EventBridge.

Topics

- Wann AWS startet und stoppt Autoshift

- Wenn ARC Übungsläufe plant, startet und beendet
- Benachrichtigung für Übungsläufe und automatische Verschiebungen
- Vorrang bei zonalen Schichten
- Beenden eines aktiven Autoshift- oder Übungslaufs für eine Ressource
- Wie wird der Verkehr wegverlagert
- Alarme für Übungsläufe
- Blockierte Daten und blockierte Fenster (UTC)

Wann AWS startet und stoppt Autoshift

Wenn Sie Zonal Autoshift für eine Ressource aktivieren, autorisieren AWS Sie, den Ressourcenverkehr für eine Anwendung bei Ereignissen in Ihrem Namen aus einer Availability Zone zu verlagern, um die Zeit bis zur Wiederherstellung zu verkürzen.

Um dies zu erreichen, verwendet Zonal Autoshift AWS Telemetrie, um so früh wie möglich zu erkennen, dass eine Beeinträchtigung der Availability Zone vorliegt, die sich möglicherweise auf Kunden auswirken könnte. Wenn ein Autoshift AWS gestartet wird, wird der Datenverkehr zu den konfigurierten Ressourcen sofort aus der beeinträchtigten Availability Zone verlagert, was sich potenziell auf Kunden auswirken könnte.

Zonal Autoshift ist eine Funktion, die für Kunden konzipiert wurde, die ihre Anwendungsressourcen für alle Availability Zones in einem vorab skaliert haben. AWS-Region Sie sollten sich nicht auf die bedarfsorientierte Skalierung verlassen, wenn ein Autoshift oder ein Übungslauf gestartet wird.

AWS beendet einen Autoshift, wenn festgestellt wird, dass die Availability Zone wiederhergestellt wurde.

Wenn ARC Übungsläufe plant, startet und beendet

ARC plant wöchentlich einen Übungslauf für eine Ressource, der etwa 30 Minuten dauert. ARC plant, startet und verwaltet Übungsläufe für jede Ressource unabhängig voneinander. ARC fasst keine Übungsläufe für Ressourcen auf demselben Konto zusammen.

Wenn ein Übungslauf für die erwartete Dauer ohne Unterbrechung fortgesetzt wird, wird er mit einem Ergebnis von gekennzeichnet`SUCCESSFUL`. Es gibt mehrere andere mögliche Ergebnisse: `FAILED`, `INTERRUPTED`, und`PENDING`. Ergebniswerte und Beschreibungen sind im Abschnitt Ergebnisse der Übungsläufe enthalten.

Es gibt einige Szenarien, in denen ARC einen Übungslauf unterbricht und beendet. Wenn beispielsweise ein Autoshift während eines Übungslaufs startet, unterbricht ARC den Übungslauf und beendet ihn. Nehmen wir als weiteres Beispiel an, dass die Ressource negativ auf einen Übungslauf reagiert und einen Alarm auslöst, den Sie zur Überwachung des Übungslaufs angegeben haben, sodass dieser in einen `ALARM` Zustand übergeht. In diesem Szenario unterbricht ARC auch den Übungslauf und beendet ihn.

Darüber hinaus gibt es mehrere Szenarien, in denen ARC keinen geplanten Übungslauf für eine Ressource startet.

Als Reaktion auf unterbrochene und blockierte Übungsläufe für eine Ressource geht ARC wie folgt vor:

- Wenn ein Übungslauf für eine Ressource unterbrochen wird, während er in Bearbeitung ist, betrachtet ARC den wöchentlichen Übungslauf als beendet und plant für die nächste Woche einen neuen Übungslauf für die Ressource. Das wöchentliche Trainingsergebnis `INTERRUPTED` entspricht diesem Szenario, nicht`FAILED`. Das Ergebnis des Übungslaufs wird `FAILED` nur dann angezeigt, wenn der Ergebnisalarm, der den Übungslauf überwacht, während des Übungslaufs in einen `ALARM` Zustand übergeht.
- Wenn beim geplanten Start eines Übungslaufs für eine Ressource eine Sperrbeschränkung besteht, startet ARC den Übungslauf nicht. ARC setzt die regelmäßige Überwachung fort, um festzustellen, ob immer noch eine oder mehrere Sperrbeschränkungen bestehen. Wenn es keine Blockierungsbeschränkungen gibt, startet ARC den Übungslauf für die Ressource.

Im Folgenden finden Sie Beispiele für Blockierungsbeschränkungen, die ARC daran hindern, einen Übungslauf für eine Ressource zu starten oder fortzusetzen:

- ARC startet oder setzt keine Übungsläufe fort, wenn gerade ein AWS Fault Injection Service Experiment läuft. Wenn ein AWS FIS Ereignis aktiv ist, obwohl ARC den Start eines Übungslaufs geplant hat, startet ARC den Übungslauf nicht. ARC überwacht während der Trainingsläufe die Blockierung von Einschränkungen, einschließlich eines AWS FIS Ereignisses. Wenn ein AWS FIS Ereignis beginnt, während ein Übungslauf aktiv ist, beendet ARC den Übungslauf und versucht erst, einen weiteren zu starten, wenn der nächste reguläre Übungslauf für die Ressource stattfindet.
- Wenn in einer Region ein aktuelles AWS Ereignis stattfindet, startet ARC keine Übungsläufe für Ressourcen und beendet aktive Übungsläufe in der Region.

Wenn der Trainingslauf ohne Unterbrechung beendet ist, plant ARC wie gewohnt den nächsten Trainingslauf in einer Woche. Wenn ein Übungslauf aufgrund einer Blockierungsbeschränkung

nicht gestartet wird, z. B. aufgrund eines AWS FIS Experiments oder eines von Ihnen angegebenen blockierten Zeitfensters, versucht ARC weiterhin, einen Übungslauf zu starten, bis der Übungslauf gestartet werden kann.

Benachrichtigungen für Übungsläufe und Autoshifts

Sie können wählen, ob Sie über Übungsläufe und automatische Verschiebungen für Ihre Ressource informiert werden möchten, indem Sie EventBridge Amazon-Benachrichtigungen einrichten. Sie können auch EventBridge Benachrichtigungen einrichten, wenn Sie Zonal Autoshift nicht für Ressourcen aktiviert haben. Dies wird als Autoshift-Observer-Benachrichtigung bezeichnet. Mit der Autoshift-Observer-Benachrichtigung werden Sie über alle Autoshifts informiert, die ARC startet, wenn eine Availability Zone potenziell beeinträchtigt ist. Beachten Sie, dass Sie diese Option in allen Bereichen konfigurieren müssen AWS-Region , über die Sie Benachrichtigungen erhalten möchten.

Die Schritte zur Aktivierung der Autoshift-Observer-Benachrichtigung finden Sie unter Zonal Autoshift aktivieren und damit arbeiten. Weitere Informationen zu Benachrichtigungsoptionen und deren Konfiguration finden Sie EventBridge unterZonal Autoshift mit Amazon verwenden EventBridge.

Vorrang für zonale Verschiebungen

Zu einem bestimmten Zeitpunkt kann nicht mehr als eine zonale Verschiebung angewendet werden, d. h. es kann nur ein Übungsbeispiel für die Ressource Zonenschicht, kundeninitiierte Zonenverschiebung, automatische Verschiebung oder Experiment durchgeführt werden. AWS FIS Wenn eine zweite Zonenverschiebung gestartet wird, bestimmt ARC anhand einer Rangfolge, welcher Typ der Zonenverschiebung für eine Ressource gilt.

Das allgemeine Prioritätsprinzip besteht darin, dass zonale Schichten, die Sie als Kunde starten, Vorrang vor anderen Schichttypen haben.

Um dies zu verdeutlichen, wird im Folgenden anhand einiger Beispielszenarien beschrieben, wie die Rangfolge funktioniert:

Der Typ der zonalen Schicht wurde angewendet	Der Typ der zonalen Verschiebung wurde eingeleitet	Ergebnis
AWS FIS Experiment	Üben, laufen	Der Übungslauf kann nicht gestartet werden, da das

Der Typ der zonalen Schicht wurde angewendet	Der Typ der zonalen Verschiebung wurde eingeleitet	Ergebnis
		AWS FIS Experiment Vorrang hat.
AWS FIS Experiment	Manuelle Zonenverschiebung	Das AWS FIS Experiment wird abgebrochen und die manuelle Zonenverschiebung wird angewendet.
AWS FIS Experiment	Zonaler Autoshift	Das AWS FIS Experiment wird abgebrochen und der zonale Autoshift wird angewendet.
AWS FIS Experiment	AWS FIS experimentieren	Das initiierte AWS FIS Experiment kann nicht gestartet werden, da bereits ein Experiment läuft, das die AWS FIS Autoshift-Aktion ausgelöst hat.
Übungslauf	Manuelle Zonenverschiebung	Der Übungslauf wird unterbrochen und auf eingestelltINTERRUPTED , und die Zonenverschiebung wird angewendet.
Übungslauf	AWS FIS experimentiere	Der Übungslauf wird unterbrochen und auf eingestelltINTERRUPTED , und das AWS FIS Experiment wird angewendet.

Der Typ der zonalen Schicht wurde angewendet	Der Typ der zonalen Verschiebung wurde eingeleitet	Ergebnis
Übungslauf	Zonaler Autoshift	Der Übungslauf wird unterbrochen und auf eingestelltINTERRUPTED , und der zonale Autoshift wird angewendet.
Manuelle Zonenverschiebung	Übungslauf	Der Übungslauf kann nicht gestartet werden.
Manuelle Zonenverschiebung	AWS FIS experimentieren	Das AWS FIS Experiment kann nicht gestartet werden oder schlägt fehl, wenn es bereits läuft.
Manuelle Zonenverschiebung	Zonaler Autoshift	Der zonale Autoshift wird ACTIVE aber nicht APPLIED auf der Ressource ausgeführt. Die manuelle Zonenverschiebung hat Vorrang.
Zonaler Autoshift	AWS FIS experimentieren	Das AWS FIS Experiment kann nicht gestartet werden oder schlägt fehl, wenn es gerade läuft.
Zonaler Autoshift	Manuelle Zonenverschiebung	Der zonale Autoshift wird zwar durchgeführt, ACTIVE aber nicht APPLIED auf der Ressource. Die manuelle Zonenverschiebung hat Vorrang.

Der Typ der zonalen Schicht wurde angewendet	Der Typ der zonalen Verschiebung wurde eingeleitet	Ergebnis
Zonaler Autoshift	Übungslauf	Der Übungslauf kann nicht gestartet werden, da der zonale Autoshift Vorrang hat.

Für die Verkehrsverlagerung, die derzeit für die Ressource gilt, ist der Status „Zonenverschiebung angewendet“ auf gesetzt. `APPLIED` Es ist jeweils nur eine Schicht `APPLIED` auf eingestellt. Andere Schichten, die gerade in Bearbeitung sind, sind auf den Status eingestelltNOT_APPLIED, haben aber weiterhin ihren `ACTIVE` Status.

Beenden eines aktiven Autoshift- oder Übungslaufs für eine Ressource

Um einen laufenden Autoshift für eine Ressource zu beenden, deaktivieren Sie den zonalen Autoshift für die Ressource.

Wenn Sie Zonal Autoshift deaktivieren, hat dies keinen Einfluss auf die Konfiguration des Übungslaufs für die Ressource. Für die Ressource finden weiterhin reguläre Übungsläufe nach demselben Zeitplan statt. Wenn Sie zusätzlich zur Deaktivierung von Autoshifts auch die Übungsläufe beenden möchten, müssen Sie die der Ressource zugeordnete Übungslaufkonfiguration löschen.

Wenn Sie eine Übungslaufkonfiguration löschen, werden keine Übungsläufe AWS mehr ausgeführt, bei denen der Verkehr für die Ressource jede Woche aus einer Availability Zone verlagert wird. Da für zonales Autoshift außerdem Übungsläufe erforderlich sind, deaktiviert diese Aktion beim Löschen einer Übungslaufkonfiguration mithilfe der ARC-Konsole auch zonales Autoshift für die Ressource. Beachten Sie jedoch, dass Sie, wenn Sie die Zonal Autoshift API verwenden, um einen Übungslauf zu löschen, zuerst Zonal Autoshift für die Ressource deaktivieren müssen.

Um einen aktiven Übungslauf zu beenden, brechen Sie den Übungslauf mit zonaler Verschiebung ab. Weitere Informationen finden Sie unter Um einen Übungslauf abzubrechen, Zonal Shift..

Wie wird der Verkehr wegverlagert

Bei Autoshifts und in der Praxis ausgeführten Zonenschichten wird der Verkehr von einer Availability Zone weggeleitet. Dabei wird derselbe Mechanismus verwendet, den ARC für vom Kunden initiierte Zonenverschiebungen verwendet. Eine fehlerhafte Zustandsprüfung führt

dazu, dass Amazon Route 53 die entsprechenden IP-Adressen für die Ressource aus dem DNS entfernt, sodass der Verkehr aus der Availability Zone umgeleitet wird. Neue Verbindungen werden jetzt stattdessen an andere Availability Zones in der weitergeleitet. AWS-Region

Wenn bei Autoshift eine Availability Zone wiederhergestellt wird und AWS beschließt, den Autoshift zu beenden, macht ARC den Zustandsprüfungsprozess rückgängig und fordert, dass die Route 53-Zustandsprüfungen rückgängig gemacht werden. Anschließend werden die ursprünglichen zonalen IP-Adressen wiederhergestellt, und wenn die Integritätsprüfungen weiterhin fehlerfrei sind, wird die Availability Zone wieder in das Routing der Anwendung aufgenommen.

Es ist wichtig, sich bewusst zu sein, dass Autoshifts nicht auf Integritätsprüfungen basieren, die den zugrunde liegenden Zustand von Load-Balancern oder Anwendungen überwachen. ARC verwendet Integritätsprüfungen, um den Verkehr von Availability Zones wegzuleiten, indem es verlangt, dass die Zustandsprüfungen auf fehlerhaft gesetzt werden, und stellt dann wieder den Normalzustand der Integritätsprüfungen wieder her, wenn ein Autoshift oder ein zonaler Shift beendet wird.

Alarme für Übungsläufe

Sie können zwei CloudWatch Alarme für Übungsläufe im zonalen Autoshift angeben. Der erste Alarm, der Ergebnisalarm, ist erforderlich. Sie sollten den Ergebnisalarm so konfigurieren, dass er den Zustand Ihrer Anwendung überwacht, wenn der Datenverkehr bei jedem 30-minütigen Übungslauf von einer Availability Zone weggeleitet wird.

Damit ein Übungslauf effektiv ist, geben Sie als Ergebnisalarm einen CloudWatch Alarm an, der Metriken für die Ressource oder Ihre Anwendung überwacht, die mit einem `ALARM` Status reagieren, wenn Ihre Anwendung durch den Verlust einer Availability Zone beeinträchtigt wird. Weitere Informationen finden Sie im Abschnitt Alarme, die Sie für Übungsläufe angeben, unterBewährte Methoden bei der Konfiguration von Zonal Autoshift.

Der Ergebnisalarm enthält auch Informationen zum Ergebnis des Übungslaufs, das ARC für jeden Übungslauf meldet. Wenn der Alarm in einen `ALARM` Zustand übergeht, wird der Übungslauf beendet und das Ergebnis des Übungslaufs wird als zurückgegeben`FAILED`. Wenn der Übungslauf den geplanten 30-minütigen Testzeitraum abschließt und der Ergebnisalarm keinen `ALARM` Status annimmt, wird das Ergebnis als zurückgegeben`SUCCEEDED`. Eine Liste aller Ergebniswerte mit Beschreibungen finden Sie im Abschnitt Ergebnisse der Übungsläufe.

Optional können Sie einen zweiten Alarm angeben, den Blockierungsalarm. Der Blockierungsalarm verhindert, dass Übungsläufe gestartet oder fortgesetzt werden, wenn sie sich

in einem bestimmten `ALARM` Zustand befinden. Dieser Alarm verhindert, dass Verkehrsschichten im Übungslauf gestartet werden, und stoppt alle laufenden Übungsläufe, wenn sich der Alarm in einem bestimmten Zustand befindet. `ALARM`

Wenn beispielsweise in einer großen Architektur mit mehreren Microservices ein Problem auftritt, möchten Sie in der Regel alle anderen Änderungen in der Anwendungsumgebung stoppen, was auch das Blockieren von Übungsläufen einschließen würde.

Blockierte Daten und blockierte Fenster (UTC)

Sie haben die Möglichkeit, Übungsläufe für bestimmte Kalenderdaten oder für bestimmte Zeitfenster, d. h. Tage und Uhrzeiten, in UTC zu blockieren.

Wenn Sie beispielsweise ein Anwendungsupdate haben, das am 1. Mai 2024 gestartet werden soll, und Sie nicht möchten, dass zu diesem Zeitpunkt durch Übungsläufe der Verkehr weggelenkt wird, können Sie ein Sperrdatum für festlegen`2024-05-01`.

Oder nehmen wir an, Sie führen drei Tage die Woche Zusammenfassungen von Geschäftsberichten durch. In diesem Szenario könnten Sie die folgenden wiederkehrenden Tage und Uhrzeiten als blockierte Fenster festlegen, z. B. in UTC:`MON-20:30-21:30 WED-20:30-21:30 FRI-20:30-21:30`.

Über Zonal Autoshift

Zonal Autoshift ist eine Funktion, mit der der Datenverkehr von AWS Anwendungsressourcen in Ihrem Namen von einer Availability Zone weggeleitet wird. AWS startet eine automatische Verschiebung, wenn die interne Telemetrie anzeigt, dass eine Beeinträchtigung der Availability Zone vorliegt, die sich möglicherweise auf Kunden auswirken könnte. Die interne Telemetrie beinhaltet Metriken aus verschiedenen Quellen, darunter dem AWS Netzwerk und den Amazon- EC2 und Elastic Load Balancing Balancing-Diensten.

Sie müssen Zonal Autoshift für unterstützte Ressourcen manuell aktivieren. AWS

Wenn Sie AWS Anwendungen auf Load Balancern in mehreren (in der Regel drei) AZs in einer Region bereitstellen und ausführen und zur Unterstützung statischer Stabilität vorab skalieren, AWS können Sie Kundenanwendungen in einer AZ schnell wiederherstellen, indem Sie den Datenverkehr mit Autoshift wegverlagern. Durch die Verlagerung des Ressourcenverkehrs auf andere AZs Standorte in der Region AWS können Dauer und Schwere potenzieller Auswirkungen reduziert werden, die durch Stromausfälle, Hardware- oder Softwareprobleme in einer AZ oder andere Beeinträchtigungen verursacht werden.

Die von ARC unterstützten Ressourcen bieten Integrationen, die die angegebene AZ als fehlerhaft kennzeichnen, was dazu führt, dass der Verkehr von der beeinträchtigten AZ weg verlagert wird.

Wenn Sie Zonal Autoshift für eine Ressource aktivieren, müssen Sie auch einen Testlauf für die Ressource konfigurieren. AWS führt etwa wöchentlich 30-minütige Übungsläufe durch, um sicherzustellen, dass Sie über genügend Kapazität verfügen, um Ihre Anwendung auch ohne eine der Availability Zones in der Region auszuführen.

Wie bei Zonal Shift gibt es einige spezifische Szenarien, in denen Zonal Autoshift den Verkehr nicht von der AZ weg verlagert. Wenn die Load Balancer-Zielgruppen beispielsweise AZs keine Instances haben oder wenn alle Instances fehlerhaft sind, befindet sich der Load Balancer in einem Fail-Open-Status und Sie können keine der Instanzen wegverlagern. AZs

Weitere Informationen zu Zonal Autoshift finden Sie unter. Zonaler Autoshift in ARC

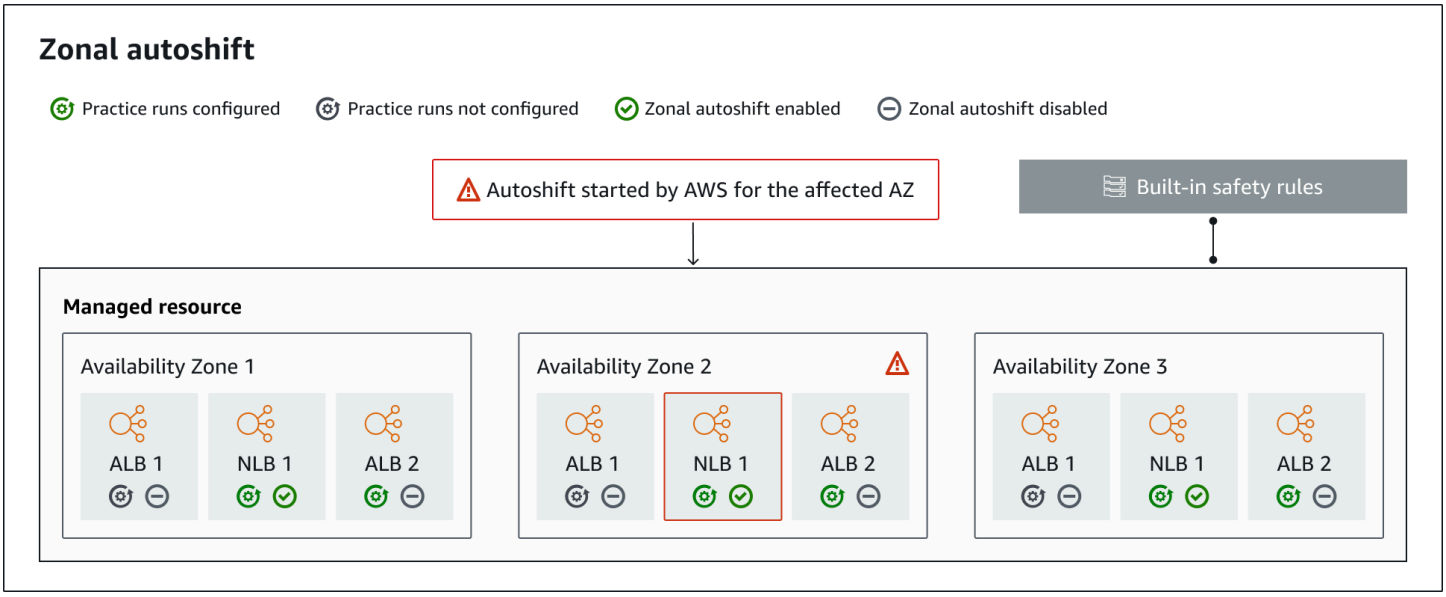
AWS-Region Verfügbarkeit von Zonal Autoshift

Zonal Shift und Zonal Autoshift sind derzeit in den AWS-Regionen hier aufgeführten Versionen verfügbar. Zonal Shift und Zonal Autoshift sind auch in den Regionen China verfügbar, d. h. in den Regionen China (Peking) und China (Ningxia). Bei Ressourcen, die Amazon Application Recovery Controller (ARC) verwenden, müssen möglicherweise zusätzliche Überlegungen angestellt werden. Weitere Informationen finden Sie unter Unterstützte Ressourcen.

Detaillierte Informationen zu regionalen Support- und Service-Endpunkten für Amazon Application Recovery Controller (ARC) finden Sie unter Amazon Application Recovery Controller (ARC) - Endpunkte und Kontingente in der Amazon Web Services General Reference.

Zonale Autoshift-Komponenten

Das folgende Diagramm zeigt ein Beispiel für eine automatische Verlagerung des Datenverkehrs von einer Availability Zone weg. AWS startet eine automatische Verschiebung, wenn die interne Telemetrie anzeigt, dass eine Beeinträchtigung der Availability Zone vorliegt, die sich möglicherweise auf Kunden auswirken könnte.



Im Folgenden sind die Komponenten der zonalen Autoshift-Funktionen in ARC aufgeführt.

Zonaler Autoshift

Zonal Autoshift verlagert den Verkehr weg zu einer Ressource, ohne dass Sie etwas unternehmen müssen. Zonal Autoshift ist eine Funktion in ARC, bei der ein Autoshift AWS gestartet wird, wenn die interne Telemetrie anzeigt, dass eine Beeinträchtigung der Availability Zone vorliegt, die sich möglicherweise auf Kunden auswirken könnte. Beachten Sie, dass in einigen Fällen Ressourcen verlagert werden können, die keine Auswirkungen haben.

Das Training läuft

Wenn Sie Zonal Autoshift für eine Ressource aktivieren, müssen Sie auch Zonal Autoshift-Übungsläufe für die Ressource konfigurieren. AWS führt eine zonale Schicht für Übungsläufe etwa wöchentlich für etwa 30 Minuten durch. Übungsläufe stellen sicher, dass Ihre Anwendung normal ausgeführt werden kann, auch wenn eine Availability Zone verloren geht. In einem Übungslauf wird der Verkehr für eine Ressource mit einer zonalen Verschiebung von einer Availability Zone weg AWS verlagert und dann, wenn der Übungslauf beendet ist, wieder zurückverlagert.

Konfiguration des Übungslaufs

Eine Konfiguration für einen Übungslauf definiert die Sperrdaten und -fenster, falls vorhanden, sowie die CloudWatch Alarme, die Sie für den Übungslauf für eine Ressource in Zonal Autoshift angeben. Sie können einen Übungslauf jederzeit bearbeiten, um blockierte Termine oder Fenster hinzuzufügen oder zu ändern oder um die Alarme für den Übungslauf zu aktualisieren.

Um Zonal Autoshift zu aktivieren, müssen Sie eine Übungslaufkonfiguration für eine Ressource eingerichtet haben. Sie können einen Übungslauf auch löschen. Um eine Übungslaufkonfiguration für eine Ressource zu löschen, muss Zonal Autoshift deaktiviert sein.

Alarm beim Übungslauf

Wenn Sie Übungsläufe konfigurieren, geben Sie CloudWatch Alarme an, die Sie auf der Grundlage Ihrer Ressourcen- und Anwendungsanforderungen in CloudWatch erstellen. Die von Ihnen angegebenen Alarme können den Start eines Übungslaufs verhindern oder einen laufenden Übungslauf beenden, falls Ihre Anwendung durch den Übungslauf beeinträchtigt wird.

Wenn ein von Ihnen festgelegter Alarm in einen bestimmten `ALARM` Zustand übergeht, beendet ARC die Zonenverschiebung für den Übungslauf, sodass der Datenverkehr für die Ressource nicht mehr von der Availability Zone wegverlagert wird.

Es gibt zwei Arten von Alarmen, die Sie für Übungsläufe angeben: einen Ergebnisalarm, um den Zustand Ihrer Ressource und Anwendung während des Übungslaufs zu überwachen, und einen Blockierungsalarm, den Sie konfigurieren können, um zu verhindern, dass Übungsläufe gestartet werden, oder um einen laufenden Übungslauf zu beenden. Der Ergebnisalarm ist erforderlich, der Blockierungsalarm ist optional.

Ergebnis des Übungslaufs

ARC meldet für jeden Übungslauf ein Ergebnis. Im Folgenden sind die möglichen Ergebnisse des Übungslaufs aufgeführt:

- AUSSTEHEND: Die Zonenverschiebung für den Übungslauf ist aktiv (läuft). Es gibt noch kein Ergebnis für eine Rückkehr.
- ERFOLGREICH: Der Ergebnisalarm hat während des Übungslaufs keinen `ALARM` Status erreicht, und der Übungslauf hat den gesamten 30-minütigen Testzeitraum abgeschlossen.
- UNTERBROCHEN: Der Übungslauf wurde aus einem Grund beendet, der nicht darauf zurückzuführen war, dass der Ergebnisalarm in einen `ALARM` Status übergegangen ist. Ein Übungslauf kann aus verschiedenen Gründen unterbrochen werden. Ein Beispiel: Ein Übungslauf, der beendet wird, weil der für den Übungslauf angegebene Blockierungsalarm in einen `ALARM` Zustand übergegangen ist, hat das Ergebnis von`INTERRUPTED`. Weitere Informationen zu den Gründen für ein `INTERRUPTED` Ergebnis finden Sie unter Ergebnisse von Übungsläufen.
- FEHLGESCHLAGEN: Der Ergebnisalarm hat während des Übungslaufs einen `ALARM` Status erreicht.

Integrierte Sicherheitsregeln

Die in ARC integrierten Sicherheitsregeln verhindern, dass mehr als eine Verkehrsverlagerung für eine Ressource gleichzeitig in Kraft ist. Das heißt, nur eine vom Kunden initiierte Zonenverschiebung, ein Übungslauf zur Zonenverschiebung oder eine automatische Verschiebung für die Ressource kann den Verkehr aktiv von einer Availability Zone weg verlagern. Wenn Sie beispielsweise eine Zonenverschiebung für eine Ressource starten, obwohl diese derzeit mit Autoshift wegverlagert ist, hat Ihre Zonenverschiebung Vorrang. Weitere Informationen finden Sie unter Ergebnisse von Übungsläufen.

Ressourcen-ID

Der Bezeichner für eine Ressource, für die zonale Autoshift aktiviert werden soll. Dabei handelt es sich um den Amazon-Ressourcennamen (ARN) für die Ressource.

Sie können Zonal Autoshift nur für Ressourcen in Ihrem Konto aktivieren, die sich in einem AWS Service befinden, der von ARC unterstützt wird.

Verwaltete Ressource

Application Load Balancer registrieren Ressourcen automatisch bei ARC für zonales Autoshift. Sie müssen die Network Load Balancer-Ressourcen für zonales Autoshift manuell aktivieren.

Ressourcenname

Der Name einer verwalteten Ressource in ARC.

Status „Angewendet“

Der Status „Anwendet“ gibt an, ob für eine Ressource eine Verkehrsverlagerung in Kraft ist. Wenn Sie Zonal Autoshift konfigurieren, kann eine Ressource über mehr als eine aktive Verkehrsverlagerung verfügen, d. h. einen Übungslauf Zonal Shift, eine vom Kunden initiierte Zonenverschiebung oder Autoshift. Es wird jedoch immer nur eine angewendet, d. h., sie ist jeweils für die Ressource wirksam. Die Verschiebung, die diesen Status hat, `APPLIED` bestimmt die Availability Zone, in die der Anwendungsdatenverkehr für eine Ressource verlagert wurde, und bestimmt, wann diese Verkehrsverlagerung endet.

Art der Schicht

Definiert den zonalen Schichttyp. Der `shiftType` kann die folgenden Werte haben:

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT

- ÜBUNGSLAUF
- FIS_EXPERIMENT

Daten- und Steuerungsebenen für zonales Autoshift

Denken Sie bei der Planung von Failover und Disaster Recovery darüber nach, wie robust Ihre Failover-Mechanismen sind. Es wird empfohlen, sicherzustellen, dass die Mechanismen, auf die Sie beim Failover angewiesen sind, hochverfügbar sind, sodass Sie sie bei Bedarf in einem Notfallszenario verwenden können. In der Regel sollten Sie, wann immer möglich, Datenebenenfunktionen für Ihre Mechanismen verwenden, um die größtmögliche Zuverlässigkeit und Fehlertoleranz zu gewährleisten. Vor diesem Hintergrund ist es wichtig zu verstehen, wie die Funktionalität eines Dienstes zwischen Steuerungsebenen und Datenebenen aufgeteilt ist und wann Sie sich darauf verlassen können, dass die Datenebene eines Dienstes extrem zuverlässig ist.

Im Allgemeinen ermöglicht Ihnen eine Steuerungsebene grundlegende Verwaltungsfunktionen wie das Erstellen, Aktualisieren und Löschen von Ressourcen im Service. Eine Datenebene stellt die Kernfunktionalität eines Dienstes bereit.

Weitere Informationen zu Datenebenen, Kontrollebenen und dazu, wie Services AWS entwickelt werden, um Hochverfügbarkeitsziele zu erreichen, finden Sie im paper Statische Stabilität mithilfe von Availability Zones in der Amazon Builders' Library.

Preise für Zonal Autoshift in ARC

Bei zonaler Autoshift wird der Datenverkehr in Ihrem Namen für unterstützte Ressourcen von einer Availability Zone weggeleitet, wenn AWS festgestellt wird, dass ein potenzielles Problem vorliegt, das sich negativ auf Kundenanwendungen auswirken kann. AWS Für die Aktivierung von Zonal Autoshift fallen keine zusätzlichen Gebühren an.

Detaillierte Preisinformationen für ARC und Preisbeispiele finden Sie unter ARC-Preise.

Bewährte Methoden bei der Konfiguration von Zonal Autoshift

Beachten Sie die folgenden bewährten Methoden und Überlegungen, wenn Sie Zonal Autoshift in Amazon Application Recovery Controller (ARC) aktivieren.

Zonal Autoshift umfasst zwei Arten von Verkehrsverschiebungen: Autoshifts und Practice Run Zonal Shifts.

- Autoshift AWS trägt dazu bei, die Zeit bis zur Wiederherstellung zu verkürzen, indem der Datenverkehr von Anwendungsressourcen bei Ereignissen in Ihrem Namen aus einer Availability Zone verlagert wird.
- Bei Übungsläufen startet ARC in Ihrem Namen eine Zonenverschiebung. Durch die Zonenverschiebung wird der Verkehr in wöchentlichem Rhythmus von einer Availability Zone für eine Ressource weg und wieder zurück verlagert. Mithilfe von Übungsläufen können Sie sicherstellen, dass Sie genügend Kapazität für Availability Zones in einer Region aufgebaut haben, sodass Ihre Anwendung den Verlust einer Availability Zone verkraften kann.

Es gibt mehrere bewährte Methoden und Überlegungen, die Sie bei Autoshifts und Übungsläufen beachten sollten. Lesen Sie sich die folgenden Themen durch, bevor Sie zonales Autoshift aktivieren oder Übungsläufe für eine Ressource konfigurieren.

Topics

- Begrenzen Sie die Zeit, in der Clients mit Ihren Endpunkten verbunden bleiben
- Skalieren Sie Ihre Ressourcenkapazität im Voraus und testen Sie die Verlagerung des Datenverkehrs
- Seien Sie sich der Ressourcentypen und Einschränkungen bewusst
- Geben Sie Alarme für Übungsläufe an
- Evaluieren Sie die Ergebnisse von Übungsläufen

Beschränken Sie die Zeit, in der Kunden mit Ihren Endpunkten verbunden bleiben

Wenn Amazon Application Recovery Controller (ARC) den Datenverkehr von einer Beeinträchtigung wegleitet, beispielsweise mithilfe von Zonal Shift oder Zonal Autoshift, ist der Mechanismus, den ARC verwendet, um Ihren Anwendungsdatenverkehr zu verlagern, ein DNS-Update. Ein DNS-Update bewirkt, dass alle neuen Verbindungen vom beeinträchtigten Standort weggeleitet werden. Clients mit bereits bestehenden offenen Verbindungen können jedoch weiterhin Anfragen an den beeinträchtigten Standort stellen, bis die Clients wieder eine Verbindung herstellen. Um eine schnelle Wiederherstellung zu gewährleisten, empfehlen wir, die Dauer zu begrenzen, für die Clients mit Ihren Endpunkten verbunden bleiben.

Wenn Sie einen Application Load Balancer verwenden, können Sie mit dieser `keepalive` Option konfigurieren, wie lange Verbindungen bestehen bleiben. Wir empfehlen Ihnen, den `keepalive` Wert zu senken, um Ihrem Ziel für die Wiederherstellungszeit Ihrer Anwendung zu entsprechen,

z. B. 300 Sekunden. Wenn Sie eine `keepalive` Zeit wählen, sollten Sie berücksichtigen, dass dieser Wert einen Kompromiss darstellt zwischen einer häufigeren Wiederherstellung der Verbindung im Allgemeinen, was sich auf die Latenz auswirken kann, und einer schnelleren Verlagerung aller Clients aus einer beeinträchtigten AZ oder Region.

Weitere Informationen zur Einstellung der `keepalive` Option für Application Load Balancer finden Sie unter der Keepalive-Dauer des HTTP-Clients im Application Load Balancer Balancer-Benutzerhandbuch.

Skalieren Sie Ihre Ressourcenkapazität vorab und testen Sie die Verlagerung des Datenverkehrs

Bei der AWS Verlagerung des Datenverkehrs von einer Availability Zone für eine Zonenschicht oder eine automatische Verschiebung ist es wichtig, dass die verbleibenden Availability Zones die erhöhten Anforderungsraten für Ihre Ressource bewältigen können. Dieses Muster wird als statische Stabilität bezeichnet. Weitere Informationen finden Sie im Whitepaper Statische Stabilität mithilfe von Availability Zones in der Amazon Builder's Library.

Wenn Ihre Anwendung beispielsweise 30 Instances benötigt, um ihre Clients zu bedienen, sollten Sie 15 Instances in drei Availability Zones bereitstellen, also insgesamt 45 Instances. Auf diese Weise AWS können Sie bei der AWS Verlagerung des Datenverkehrs von einer Availability Zone weg — mit Autoshift oder während eines Übungslaufs — die Clients Ihrer Anwendung weiterhin mit den verbleibenden insgesamt 30 Instances in zwei Availability Zones bedienen.

Die zonale Autoshift-Funktion in ARC hilft Ihnen bei der schnellen Wiederherstellung nach AWS Ereignissen in einer Availability Zone, wenn Sie eine Anwendung mit Ressourcen haben, die so skaliert sind, dass sie bei Verlust einer Availability Zone normal funktionieren. Bevor Sie Zonal Autoshift für eine Ressource aktivieren, skalieren Sie Ihre Ressourcenkapazität in allen konfigurierten Availability Zones in einer. AWS-Region Starten Sie dann Zonenverschiebungen für die Ressource, um zu testen, ob Ihre Anwendung weiterhin normal läuft, wenn der Verkehr von einer Availability Zone weg verlagert wird.

Nachdem Sie mit Zonal Shifts getestet haben, aktivieren Sie Zonal Autoshift und konfigurieren Sie Übungsläufe für Anwendungsressourcen. Regelmäßige Testläufe mit zonalem Autoshift helfen Ihnen, kontinuierlich sicherzustellen, dass Ihre Kapazität weiterhin angemessen skaliert wird. Bei ausreichender Kapazität in allen Availability Zones kann Ihre Anwendung während einer automatischen Verschiebung weiterhin ohne Unterbrechung Clients bedienen.

Weitere Informationen zum Starten einer Zonenverschiebung für eine Ressource finden Sie unter. Zonenverschiebung in ARC

Seien Sie sich der Ressourcentypen und Einschränkungen bewusst

Zonal Autoshift unterstützt die Verlagerung des Datenverkehrs aus einer Availability Zone für alle Ressourcen, die von Zonal Shift unterstützt werden. In einigen spezifischen Ressourcenszenarien verlagert Zonal Autoshift den Verkehr nicht von einer Availability Zone in eine Autoshift.

Wenn die Load Balancer-Zielgruppen in den Availability Zones beispielsweise keine Instances haben oder wenn alle Instances fehlerhaft sind, befindet sich der Load Balancer in einem Fail-Open-Status. Wenn in diesem Szenario ein Autoshift für einen Load Balancer AWS gestartet wird, ändert ein Autoshift nicht, welche Availability Zones der Load Balancer verwendet, da sich der Load Balancer bereits in einem Fail-Open-Status befindet. Dieses Verhalten wird erwartet. Autoshift kann nicht dazu führen, dass eine Availability Zone fehlerhaft ist, und dass der Verkehr in die anderen Availability Zones verlagert wird, wenn alle Availability Zones ausfallen, AWS-Region wenn alle Availability Zones ausfallen (fehlerhaft).

Ein zweites Szenario ist, wenn ein Autoshift für einen Application Load Balancer AWS gestartet wird, der ein Endpunkt für einen Accelerator ist. AWS Global Accelerator Wie bei Zonal Shift wird Autoshift für Application Load Balancers, die Endpunkte von Acceleratoren in Global Accelerator sind, nicht unterstützt.

Einzelheiten zu den unterstützten Ressourcen, einschließlich aller Anforderungen und Ausnahmen, die Sie beachten sollten, finden Sie unter. Unterstützte Ressourcen

Geben Sie Alarme für Übungsläufe an

Sie konfigurieren mindestens einen Alarm (den Ergebnisalarm) für Übungsläufe mit zonaler Autoshift. Optional können Sie auch einen zweiten Alarm (den Blockierungsalarm) konfigurieren.

Wenn Sie die CloudWatch Alarme berücksichtigen, die Sie für Übungsläufe für Ihre Ressource konfigurieren, sollten Sie Folgendes berücksichtigen:

- Für den Ergebnisalarm, der erforderlich ist, empfehlen wir, einen CloudWatch Alarm so zu konfigurieren, dass er in einen `ALARM` Zustand übergeht, in dem die Metriken für die Ressource oder Ihre Anwendung darauf hinweisen, dass die Verlagerung des Datenverkehrs von der Availability Zone weg die Leistung beeinträchtigt. Sie können beispielsweise einen Schwellenwert für die Anforderungsraten für Ihre Ressource festlegen und dann einen Alarm so konfigurieren, dass er in einen `ALARM` Status wechselt, wenn der Schwellenwert überschritten wird. Sie sind dafür verantwortlich, einen geeigneten Alarm zu konfigurieren, der AWS dazu führt, dass der Übungslauf beendet und ein `FAILED` Ergebnis zurückgegeben wird.
- Wir empfehlen Ihnen, das AWS Well Architected Framework zu befolgen, das Ihnen empfiehlt, wichtige Leistungsindikatoren (KPIs) als CloudWatch Alarme zu implementieren. Wenn Sie dies

tun, können Sie diese Alarme verwenden, um einen zusammengesetzten Alarm zu erstellen, der als Sicherheitsauslöser verwendet werden kann, um zu verhindern, dass Übungsläufe gestartet werden, wenn diese dazu führen könnten, dass Ihre Anwendung einen KPI verfehlt. Wenn sich der Alarm nicht mehr im `ALARM` Status befindet, startet ARC Übungsläufe, wenn das nächste Mal ein Übungslauf für die Ressource geplant ist.

- Wenn Sie den Alarm zum Sperren von Übungsläufen konfigurieren, können Sie sich dafür entscheiden, eine bestimmte Metrik nachzuverfolgen, anhand derer Sie angeben, dass Sie nicht möchten, dass ein Übungslauf gestartet werden soll.
- Zum Üben von Alarmen geben Sie den Amazon-Ressourcennamen (ARN) für jeden Alarm an, den Sie zuerst in Amazon konfigurieren müssen CloudWatch. Bei den von Ihnen angegebenen CloudWatch Alarmen kann es sich um zusammengesetzte Alarme handeln, sodass Sie mehrere Messwerte und Prüfungen für Ihre Anwendung und Ressource einbeziehen können, sodass der Alarm in einen bestimmten `ALARM` Status übergeht. Weitere Informationen finden Sie unter Kombinieren von Alarmen im CloudWatch Amazon-Benutzerhandbuch.
- Stellen Sie sicher, dass sich die CloudWatch Alarme, die Sie für Übungsläufe angeben, in derselben Region befinden wie die Ressource, für die Sie einen Übungslauf konfigurieren.

Bewerten Sie die Ergebnisse von Übungsläufen

ARC meldet für jeden Übungslauf ein Ergebnis. Bewerten Sie nach einem Übungslauf das Ergebnis und entscheiden Sie, ob Sie Maßnahmen ergreifen müssen. Beispielsweise müssen Sie möglicherweise die Kapazität skalieren oder die Konfiguration für einen Alarm anpassen.

Im Folgenden sind die möglichen Ergebnisse des Übungslaufs aufgeführt:

- ERFOLGREICH: Der Ergebnisalarm hat während des Übungslaufs keinen `ALARM` Status erreicht, und der Übungslauf hat den gesamten 30-minütigen Testzeitraum abgeschlossen.
- FEHLGESCHLAGEN: Der Ergebnisalarm hat während des Übungslaufs einen `ALARM` Status erreicht.
- UNTERBROCHEN: Der Übungslauf wurde aus einem Grund beendet, der nicht darauf zurückzuführen war, dass der Ergebnisalarm in einen `ALARM` Status übergegangen ist. Ein Übungslauf kann aus einer Vielzahl von Gründen unterbrochen werden, unter anderem aus den folgenden Gründen:
  - Der Übungslauf wurde beendet, weil in der Region ein Autoshift AWS gestartet wurde AWS-Region oder weil in der Region ein Alarm aufgetreten ist.
  - Der Übungslauf wurde beendet, weil die Konfiguration des Übungslaufs für die Ressource gelöscht wurde.

  - Der Übungslauf wurde beendet, weil eine vom Kunden initiierte Zonenverschiebung für die Ressource in der Availability Zone gestartet wurde, von der der Übungslauf mit der Zonenschicht den Verkehr wegverlagerte.
  - Der Übungslauf wurde beendet, weil auf einen CloudWatch Alarm, der für die Konfiguration des Übungslaufs angegeben wurde, nicht mehr zugegriffen werden kann.
  - Der Übungslauf wurde beendet, weil der für den Übungslauf angegebene Blockierungsalarm in einen `ALARM` Status übergegangen ist.
  - Der Übungslauf wurde aus einem unbekannten Grund beendet.
  - Der Übungslauf wurde beendet, weil ein zonaler Autoshift mit Vorrang eingeleitet wurde. Siehe Priorität für zonale Verschiebungen.
- AUSSTEHEND: Der Übungslauf ist aktiv (läuft). Es gibt noch kein Ergebnis für eine Rückkehr.

Zonale Autoshift-API-Operationen

In der folgenden Tabelle sind ARC-API-Operationen aufgeführt, die Sie mit zonalem Autoshift verwenden können. Beispiele für die Verwendung von zonalen Autoshift-API-Operationen mit dem finden Sie unter. AWS CLI

Beispiele für die Verwendung gängiger zonaler Autoshift-API-Operationen mit dem finden Sie unter. AWS Command Line InterfaceBeispiele für die Verwendung von AWS CLI mit zonalem Autoshift

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Erstellen Sie eine Konfiguration für Übungsläufe	Siehe Zonal Autoshift aktivieren oder deaktivieren	Siehe CreatePracticeRunConfiguration
Löschen Sie eine Übungslaufkonfiguration	Siehe Konfiguration, Bearbeitung oder Löschung einer Übungslaufkonfiguration	Siehe DeletePracticeRunConfiguration
Autoshift auflisten	Siehe Zonaler Autoshift in ARC	Siehe ListAutoshifts
Listet Ressourcen für zonales Autoshift auf	Siehe Unterstützte Ressourcen	Siehe ListManagedResources

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Holen Sie sich Ressourcen für Zonal Autoshift	Siehe Unterstützte Ressourcen	Siehe GetManagedResource
Bearbeiten Sie eine Konfiguration für einen Übungslauf	Siehe Konfiguration, Bearbeitung oder Löschung einer Übungslaufkonfiguration	Siehe UpdatePracticeRunConfiguration
Aktivieren oder deaktivieren Sie Zonal Autoshift	Siehe Zonal Autoshift aktivieren oder deaktivieren	Siehe UpdateZonalAutoshiftConfiguration
Aktivieren oder deaktivieren Sie die Autoshift-Observer-Benachrichtigung	Siehe Zonal Autoshift aktivieren und damit arbeiten	Siehe UpdateAutoshiftObserverNotificationStatus

Beispiele für die Verwendung von AWS CLI mit zonalem Autoshift

In diesem Abschnitt werden einfache Anwendungsbeispiele für die Arbeit mit zonalem Autoshift vorgestellt, wobei die Verwendung von API-Vorgängen AWS Command Line Interface zur Verwendung der zonalen Autoshift-Funktion in Amazon Application Recovery Controller (ARC) verwendet wird. Die Beispiele sollen Ihnen helfen, ein grundlegendes Verständnis für die Arbeit mit zonalem Autoshift mithilfe der CLI zu entwickeln.

Zonal Autoshift ist eine Funktion in ARC. Mit Zonal Autoshift autorisieren AWS Sie, den Datenverkehr für unterstützte Anwendungsressourcen bei Ereignissen in Ihrem Namen aus einer Availability Zone zu verlagern, um die Zeit bis zur Wiederherstellung zu verkürzen. Zonal Autoshift umfasst Testläufe, bei denen der Datenverkehr auch von Availability Zones weggeleitet wird. So können Sie kontinuierlich überprüfen, ob Autoshift für Ihre Anwendung sicher ist.

Weitere Informationen finden Sie unter Unterstützte Ressourcen.

In diesem Abschnitt werden anhand der folgenden Beispiele veranschaulicht, wie Sie mit Zonal Autoshift beginnen und wie Sie damit arbeiten können:

- Erstellen Sie eine Übungslaufkonfiguration für eine Ressource.
- Aktivieren und deaktivieren Sie Autoshift für eine Ressource.

- Beenden Sie einen laufenden Übungslauf, indem Sie die mit dem Übungslauf begonnene Zonenschicht abbrechen.
- Beenden Sie eine laufende automatische Verschiebung, indem Sie die Funktion für die zonale automatische Verschiebung für eine Ressource deaktivieren.
- Bearbeiten Sie eine Übungslaufkonfiguration für eine Ressource, um die angegebenen Alarme oder Sperrdaten oder -fenster zu ändern.
- Löscht eine Übungslaufkonfiguration für eine Ressource.

Weitere Informationen zur Verwendung von finden Sie in der AWS CLI Befehlsreferenz. AWS CLI Eine Liste der zonalen Autoshift-API-Aktionen und Links zu weiteren Informationen finden Sie unter. Zonale Autoshift-API-Operationen

Erstellen Sie eine Konfiguration für den Übungslauf

Bevor Sie Zonal Autoshift für eine Ressource aktivieren können, müssen Sie eine Übungslaufkonfiguration für die Ressource erstellen, um Optionen für die erforderlichen Übungsläufe auszuwählen. Sie erstellen eine Übungslaufkonfiguration für eine Ressource mit der CLI, indem Sie den `create-practice-run-configuration` Befehl verwenden.

Beachten Sie Folgendes, wenn Sie eine Übungslaufkonfiguration für eine Ressource erstellen:

- Der einzige unterstützte Alarmtyp ist derzeit`CLOUDWATCH`.
- Sie müssen Alarme verwenden, die sich in derselben Form befinden AWS-Region , in der Ihre Ressource bereitgestellt wird.
- Die Angabe eines Ergebnisalarms ist erforderlich. Die Angabe eines Blockierungsalarms ist optional.
- Die Angabe von gesperrten Daten oder blockierten Fenstern ist optional.

Sie erstellen eine Übungslaufkonfiguration mit der CLI, indem Sie den `create-practice-run-configuration` Befehl verwenden.

Um beispielsweise eine Übungslaufkonfiguration für eine Ressource zu erstellen, verwenden Sie einen Befehl wie den folgenden:

```
aws arc-zonal-shift create-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
```

```
      --outcome-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
MyAppHealthAlarm \
      --blocking-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
BlockWhenALARM \
      --blocked-dates 2023-12-01 --blocked-windows Mon:10:00-Mon:10:30
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                  {
              "type": "CLOUDWATCH",
              "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
       "blockedWindows": [
           "Mon:10:00-Mon:10:30"
       ],
       "blockedDates": [
           "2023-12-01"
       ]
}
```

Aktivieren oder deaktivieren Sie Autoshift

Sie aktivieren oder deaktivieren Autoshift für eine Ressource, indem Sie den zonalen Autoshift-Status mit der CLI aktualisieren. Verwenden Sie den Befehl, um den zonalen Autoshift-Status zu ändern. `update-zonal-autoshift-configuration`

Um beispielsweise Autoshift für eine Ressource zu aktivieren, verwenden Sie einen Befehl wie den folgenden:

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="ENABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "ENABLED"
}
```

Brechen Sie einen laufenden Autoshift-Vorgang ab

Um eine laufende automatische Verschiebung für eine Ressource abzubrechen, deaktivieren Sie die Funktion Zonal Autoshift. Dies ist derselbe Befehl, mit dem Sie den zonalen Autoshift generell deaktivieren. Wenn Sie also den zonalen Autoshift deaktivieren, um einen laufenden Autoshift abzubrechen, wird die Ressource auch nicht von future Autoshifts beeinflusst. Sie können den zonalen Autoshift jederzeit aktualisieren, um ihn wieder zu aktivieren.

Beachten Sie, dass Sie Zonal Autoshift für eine Ressource deaktivieren können, ohne die Übungslaufkonfiguration für die Ressource zu löschen.

Um einen Autoshift mit der CLI abzubrechen, deaktivieren Sie Zonal Autoshift mit dem Befehl. `update-zonal-autoshift-configuration` Um beispielsweise einen Autoshift für eine Ressource zu beenden, verwenden Sie einen Befehl wie den folgenden:

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Brechen Sie einen laufenden Übungslauf ab

Sie können einen laufenden Übungslauf mit der CLI abbrechen, indem Sie die zonale Schicht abbrechen, die der Übungslauf für die Ressource gestartet hat. Verwenden Sie den Befehl, um einen Übungslauf abzubrechen. `cancel-zonal-shift`

Um beispielsweise einen Übungslauf für eine Ressource abzubrechen, verwenden Sie einen Befehl wie den folgenden:

```
aws arc-zonal-shift cancel-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2024-11-15T10:35:42+00:00,
    "startTime": 2024-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Practice Run Started"
}
```

Bearbeiten Sie die Konfiguration eines Übungslaufs

Sie können eine Übungslaufkonfiguration für eine Ressource mit der CLI bearbeiten, um verschiedene Konfigurationsoptionen zu aktualisieren, z. B. die Alarme für Übungsläufe zu ändern oder die gesperrten Daten oder blockierten Fenster zu aktualisieren, wenn ARC keine Übungsläufe startet. Verwenden Sie den `update-practice-run-configuration` Befehl, um eine Konfiguration für Übungsläufe zu bearbeiten.

Beachten Sie Folgendes, wenn Sie eine Übungslaufkonfiguration für eine Ressource bearbeiten:

- Der einzige unterstützte Alarmtyp ist derzeit`CLOUDWATCH`.
- Sie müssen Alarme verwenden, die sich in derselben Form befinden AWS-Region , in der Ihre Ressource bereitgestellt wird.
- Die Angabe eines Ergebnisalarms ist erforderlich. Die Angabe eines Blockierungsalarms ist optional.
- Die Angabe von gesperrten Daten oder blockierten Fenstern ist optional.

- Die von Ihnen angegebenen gesperrten Daten oder gesperrten Fenster ersetzen alle vorhandenen Werte.

Um beispielsweise eine Übungslaufkonfiguration für eine Ressource zu bearbeiten und ein neues Sperrdatum anzugeben, verwenden Sie einen Befehl wie den folgenden:

```
aws arc-zonal-shift update-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --blocked-dates 2024-03-01
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                   {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
       "blockedWindows": [
           "Mon:10:00-Mon:10:30"
       ],
       "blockedDates": [
           "2024-03-01"
       ]
}
```

Löschen Sie eine Konfiguration für einen Übungslauf

Sie können eine Übungslaufkonfiguration für eine Ressource löschen, müssen aber zuerst die zonale automatische Verschiebung für die Ressource deaktivieren. Für eine Ressource ist eine Übungslaufkonfiguration erforderlich, damit zonales Autoshift aktiviert werden kann. Durch regelmäßige Übungsläufe können Sie sicherstellen, dass Ihre Anwendung auch ohne eine Availability Zone normal ausgeführt werden kann.

Um eine Übungslaufkonfiguration mithilfe der CLI zu löschen, deaktivieren Sie zunächst Zonal Autoshift, falls erforderlich, mit dem `update-zonal-autoshift` Befehl. Verwenden Sie dann den Befehl, um die Konfiguration des Übungslaufs zu löschen. `delete-practice-run-configuration`

Deaktivieren Sie zunächst Zonal Autoshift für die Ressource, indem Sie einen Befehl wie den folgenden verwenden:

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Löschen Sie dann die Konfiguration für den Übungslauf, indem Sie einen Befehl wie den folgenden verwenden:

```
aws arc-zonal-shift delete-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890"
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "TestResource",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Zonal Autoshift aktivieren und damit arbeiten

Dieser Abschnitt enthält Verfahren für die Arbeit mit zonalen Autoshifts in Amazon Application Recovery Controller (ARC), darunter das Aktivieren und Deaktivieren von zonalem Autoshift, das Konfigurieren von Übungsläufen, das Abbrechen laufender Übungsläufe und das Aktivieren von Autoshift-Observer-Benachrichtigungen.

Zonal Autoshift aktivieren oder deaktivieren

In den Schritten in diesem Abschnitt wird erklärt, wie Sie Zonal Autoshift auf der Amazon Application Recovery Controller (ARC) -Konsole aktivieren oder deaktivieren. Informationen zum programmgesteuerten Arbeiten mit Zonal Autoshift finden Sie im Referenzhandbuch zur Zonal Shift and Zonal Autoshift API.

Wenn Zonal Autoshift aktiviert ist, autorisieren Sie, den Datenverkehr von Anwendungsressourcen bei Ereignissen in Ihrem Namen aus einer Availability Zone AWS zu verlagern, um die Zeit bis zur Wiederherstellung zu verkürzen.

Um Zonal Autoshift zu aktivieren oder zu deaktivieren

1. Öffnen Sie die ARC-Konsole unter. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. Wählen Sie unter Multi-AZ die Option Zonal Autoshift.
3. Wählen Sie unter Resource Zonal Autoshift Configurations eine Ressource aus.
4. Wählen Sie im Menü Aktionen die Option Zonal Autoshift aktivieren oder Zonal Autoshift deaktivieren aus und folgen Sie dann den Anweisungen, um das Update abzuschließen.

Wenn für die Ressource keine Konfiguration für den Übungslauf verfügbar ist, ist Zonal Autoshift aktivieren nicht verfügbar. Um eine Übungslaufkonfiguration zu konfigurieren und Zonal Autoshift zu aktivieren, wählen Sie Configure Zonal Autoshift.

Konfiguration, Bearbeitung oder Löschung einer Übungslaufkonfiguration

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Übungslaufkonfiguration auf der Amazon Application Recovery Controller (ARC) -Konsole bearbeiten oder löschen. Informationen zur programmgesteuerten Arbeit mit Zonal Autoshift, einschließlich Änderungen an den Konfigurationen für Übungsläufe, finden Sie im Referenzhandbuch für Zonal Shift und Zonal Autoshift API.

Wenn Sie eine Konfiguration für den Übungslauf in der Konsole löschen, ist Zonal Autoshift deaktiviert. Bevor Sie eine Übungslaufkonfiguration mit einem API-Vorgang löschen können, müssen Sie Zonal Autoshift deaktivieren. Sie können einen Übungslauf konfigurieren, ohne Zonal Autoshift zu aktivieren. Damit Zonal Autoshift für eine Ressource aktiviert werden kann, müssen Sie jedoch einen Übungslauf für die Ressource konfiguriert haben.

Um einen Übungslauf zu konfigurieren

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie unter Multi-AZ die Option Zonal Autoshift.
3. Wählen Sie Configure Zonal Autoshift aus.
4. Wählen Sie eine Ressource aus, die für Zonal Autoshift konfiguriert werden soll.
5. Deaktivieren Sie Zonal Autoshift, wenn Sie bei einem Ereignis keinen Autoshift für eine Ressource starten möchten AWS . AWS Wenn Sie möchten, können Sie mit dem Assistenten fortfahren, um eine Konfiguration für einen Übungslauf zu konfigurieren, ohne Autoshift zu aktivieren.
6. Wählen Sie Optionen für Übungsläufe für die Ressource aus. Bei Alarmen können Sie wie folgt vorgehen:

   - (Erforderlich) Geben Sie einen Ergebnisalarm an, um Übungsläufe für diese Ressource zu überwachen.
   - (Optional) Geben Sie einen Blockierungsalarm für Übungsläufe für diese Ressource an.

   Weitere Informationen finden Sie im Abschnitt Alarme, die Sie für Übungsläufe angeben, unterBewährte Methoden bei der Konfiguration von Zonal Autoshift.
7. Geben Sie optional gesperrte Daten und gesperrte Fenster an. Wählen Sie Daten oder Fenster (Tage und Uhrzeiten), um zu verhindern, dass ARC Übungsläufe für diese Ressource startet. Alle Daten und Uhrzeiten sind in UTC angegeben.
8. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Bestätigungsnotiz gelesen haben.
9. Wählen Sie Erstellen aus.

Um eine Übungslaufkonfiguration zu bearbeiten

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie unter Multi-AZ die Option Zonal Autoshift.
3. Wählen Sie unter Resource Zonal Autoshift Configurations eine Ressource aus.
4. Wählen Sie im Menü Aktionen die Option Übungslaufkonfiguration bearbeiten aus.
5. Nehmen Sie Änderungen an der Konfiguration des Übungslaufs vor, um eine oder mehrere der folgenden Aktionen auszuführen:

   - Bei Alarmen können Sie wie folgt vorgehen:
     - Für den Blockierungsalarm können Sie einen Alarm hinzufügen, den Alarm löschen oder einen anderen Blockierungsalarm angeben.
     - Für den Ergebnisalarm, der Übungsläufe überwacht, können Sie einen anderen CloudWatch Alarm angeben, der verwendet werden soll. Ergebnisalarme sind erforderlich, sodass Sie den Ergebnisalarm nicht löschen können.
   - Für gesperrte Daten und blockierte Fenster können Sie neue Daten oder Tage und Uhrzeiten hinzufügen oder vorhandene Daten oder Tage und Uhrzeiten entfernen oder aktualisieren. Alle Daten und Uhrzeiten sind in UTC angegeben.
6. Wählen Sie Speichern.

Um eine Übungslaufkonfiguration zu löschen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie unter Multi-AZ die Option Zonal Autoshift.
3. Wählen Sie unter Resource Zonal Autoshift Configurations eine Ressource aus.
4. Wählen Sie im Menü Aktionen die Option Übungslaufkonfiguration löschen aus.
5. Geben Sie im modalen Bestätigungsdialogfeld den Text ein`Delete`, und wählen Sie dann Löschen aus.

   Beachten Sie, dass durch das Löschen einer Übungslaufkonfiguration in der Konsole auch die zonale automatische Verschiebung für die Ressource deaktiviert wird. Für Zonal Autoshift muss ein Übungslauf für die Ressource konfiguriert werden.

Um einen Übungslauf abzubrechen, Zonal Shift.

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Zonenverschiebung auf der Amazon Application Recovery Controller (ARC) -Konsole stornieren. Informationen zum programmgesteuerten Arbeiten mit Zonal Shift und Zonal Autoshift finden Sie im Referenzhandbuch zur Zonal Shift and Zonal Autoshift API.

Sie können Zonenverschiebungen, die Sie selbst initiieren, stornieren. Sie können auch Zonenverschiebungen stornieren, die für eine Ressource im Rahmen eines Übungslaufs für zonales Autoshift AWS gestartet werden.

Um einen Übungslauf abzubrechen, Zonal Shift

1. Öffnen Sie die ARC-Konsole unter. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. Wählen Sie unter Multi-AZ die Option Zonal Shift.
3. Wählen Sie eine Zonenschicht aus, die Sie stornieren möchten, und wählen Sie dann Zonenschicht stornieren aus.
4. Wählen Sie im modalen Bestätigungsdialogfeld die Option Bestätigen.

Autoshift-Observer-Benachrichtigung aktivieren oder deaktivieren

Sie können Zonal Autoshift so konfigurieren, dass Sie über Amazon benachrichtigt werden, wenn ein Autoshift AWS gestartet wird EventBridge, um den Verkehr von einer potenziell beeinträchtigten Availability Zone weg zu verlagern. Sie müssen diese Option in allen Bereichen konfigurieren, über AWS-Region die Sie Benachrichtigungen erhalten möchten. Sie müssen keine bestimmten Ressourcen mit zonalem Autoshift konfigurieren, um diese separaten Benachrichtigungen zu aktivieren. Weitere Informationen finden Sie unter Zonal Autoshift mit Amazon verwenden EventBridge.

In den Schritten in diesem Abschnitt wird erklärt, wie Sie die Autoshift-Observer-Benachrichtigung mithilfe der Amazon Application Recovery Controller (ARC) -Konsole aktivieren. Informationen zur programmgesteuerten Arbeit mit Zonal Autoshift finden Sie im Referenzhandbuch zu Zonal Shift and Zonal Autoshift API.

So aktivieren oder deaktivieren Sie die Autoshift-Observer-Benachrichtigung

1. Öffnen Sie die ARC-Konsole unter. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. Wählen Sie unter Erste Schritte die Option Autoshift-Observer-Benachrichtigung aktivieren aus.
3. Wählen Sie im Bestätigungsdialogfeld die Option Beobachterbenachrichtigung aktivieren aus.

Testen von Zonal Autoshift mit AWS FIS

Sie können AWS Fault Injection Service damit Experimente einrichten und durchführen, die Ihnen helfen, reale Bedingungen zu simulieren, wie z. B. das Szenario AZ-Verfügbarkeit: Stromunterbrechung, in dem demonstriert wird, was passiert, wenn ein zonaler Autoshift auf Ihren Ressourcen, für die Autoshift aktiviert ist, während einer potenziell weit verbreiteten AZ-Beeinträchtigung AWS gestartet wird.

Mit der Aktion „`aws:arc:start-zonal-autoshift`Wiederherstellung starten“ können Sie demonstrieren, wie AWS während der Ausführung des AZ-Verfügbarkeitsszenarios der Verkehr für Ressourcen, die für zonales Autoshift aktiviert sind, automatisch von einer potenziell beeinträchtigten AZ weggeleitet und auf einen fehlerfreien Zustand AZs in derselben AWS Region umgeleitet wird.

Sie können die AWS FIS Szenariobibliothek beispielsweise verwenden, um eine Beeinträchtigung der AZ aufgrund einer Stromunterbrechung zu simulieren. In diesem Experiment verlagert die Wiederherstellungsaktion fünf Minuten nach Beginn der AZ-Stromunterbrechung `aws:arc:start-zonal-autoshift` automatisch den Ressourcenverkehr für die verbleibenden 25 Minuten der Stromunterbrechung von der angegebenen AZ weg, um zu demonstrieren, wie Autoshift ausgelöst würde, wenn eine potenzielle weitreichende AZ-Beeinträchtigung vorliegt. Nach Ablauf dieser Dauer wird der Verkehr nach Abschluss des Experiments wieder auf die ursprüngliche AZ umgestellt, was eine vollständige Wiederherstellung des Stromausfalls, das sich auf diese AZ ausgewirkt hat, zeigt.

AWS FIS Experimente unterscheiden sich von zonalen Autoshift-Übungsläufen darin, dass ARC während der Übungsläufe den Verkehr für Ihre Ressource von einer AZ weg verlagert. Dies ist Teil eines normalen Prozesses, um sicherzustellen, dass Ihre Anwendung den Verlust einer AZ toleriert. Es zeigt jedoch während eines AWS FIS Experiments eine Beeinträchtigung der AZ und AWS FIS zeigt, wie Autoshift für Ihre Ressourcen, für die Autoshift aktiviert ist, in Ihrem Namen ausgelöst wird, und die automatische Verschiebung dann abbricht, wenn die Beeinträchtigung behoben ist. Weitere Informationen zu Übungsläufen finden Sie unter Funktionsweise von zonalem Autoshift und Übungsläufen

Sie können eine von AWS FIS initiierte zonale Schicht nicht aktualisieren, solange sie ausgeführt wird. Wenn Sie eine zonale Schicht außerhalb von stornieren, wird das Experiment beendet. AWS FIS AWS FIS

Zu einem bestimmten Zeitpunkt kann nicht mehr als eine zonale Schicht angewendet werden, d. h. es kann nur ein Übungslauf für die Ressource Zonenverschiebung, kundeninitiierte Zonenverschiebung, Autoshift oder Experiment durchgeführt werden. AWS FIS Wenn eine zweite Zonenverschiebung gestartet wird, bestimmt ARC anhand einer Rangfolge, welcher Typ der Zonenverschiebung für eine Ressource gilt. Weitere Informationen zur Rangfolge zonaler Verschiebungen finden Sie unter Priorität für zonale Verschiebungen.

Weitere Informationen zu AWS FIS Wiederherstellungsaktionen finden Sie unter der AWS FIS Wiederherstellungsaktion im Benutzerhandbuch.AWS Fault Injection Service

Protokollierung und Überwachung für zonales Autoshift in Amazon Application Recovery Controller (ARC)

Sie können Amazon EventBridge für die Überwachung von zonalem Autoshift in Amazon Application Recovery Controller (ARC) verwenden AWS CloudTrail , um Muster zu analysieren und Probleme zu beheben.

Themen

- Protokollieren von zonalen Autoshift-API-Aufrufen mit AWS CloudTrail
- Zonal Autoshift mit Amazon verwenden EventBridge

Protokollieren von zonalen Autoshift-API-Aufrufen mit AWS CloudTrail

Zonal Autoshift for ARC ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ARC ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Zonal Shift als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der ARC-Konsole und Codeaufrufen an die ARC-API-Operationen für Zonal Shift.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Zonenverschiebungen. 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 CloudTrail, die an ARC für die Zonenverschiebung gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zum zonalen Autoshift finden Sie unter CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in ARC für Zonal Autoshift eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen. AWS-Konto Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für zonales Autoshift in ARC, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle ARC-Aktionen werden vom Routing Control API Reference Guide für Amazon Application Recovery Controller protokolliert CloudTrail und sind im Routing Control API Reference Guide dokumentiert. Beispielsweise generieren Aufrufe der `StartZonalShift` und `ListManagedResources` -Aktionen Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

ARC-Ereignisse im Ereignisverlauf anzeigen

CloudTrail ermöglicht es Ihnen, aktuelle Ereignisse im Event-Verlauf einzusehen. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Grundlegendes zu Einträgen in zonalen Autoshift-Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListManagedResources` Aktion für Zonal Autoshift demonstriert.


```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
```

```
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:14:41Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

Zonal Autoshift mit Amazon verwenden EventBridge

Mit Amazon können Sie ereignisgesteuerte Regeln einrichten EventBridge, die Ihre zonalen Autoshift-Ressourcen überwachen und Zielaktionen einleiten, die andere Dienste nutzen. AWS Sie können beispielsweise eine Regel für das Versenden von E-Mail-Benachrichtigungen festlegen, indem Sie ein Amazon SNS SNS-Thema signalisieren, wenn ein Übungslauf für Zonal Autoshift gestartet wird.

Sie können in Amazon Regeln erstellen EventBridge , um auf zonales Autoshift zu reagieren. Ein Ereignis für zonales Autoshift gibt Statusinformationen zu Übungsläufen oder Autoshifts an, z. B. wenn ein Übungslauf gestartet wird. Sie können Zonal Autoshift so konfigurieren, dass Sie über zonale Autoshift-Ereignisse für Ressourcen informiert werden, die Sie für den Service aktivieren.

Sie können zusätzlich zu oder anstelle von anderen Benachrichtigungen auch die Autoshift-Observer-Benachrichtigung aktivieren, die ein Benachrichtigungsereignis ausgibt, wenn ein Autoshift für eine potenziell beeinträchtigte Availability Zone AWS gestartet wird. Die Autoshift-Observer-Benachrichtigung unterscheidet sich von Benachrichtigungen, die Sie erhalten, wenn der Datenverkehr für Ressourcen, die Sie für zonales Autoshift aktiviert haben, von einer Availability

Zone weg verlagert wird. Sie müssen keine Ressourcen mit zonalem Autoshift konfigurieren, um die Autoshift-Observer-Benachrichtigung zu aktivieren. Weitere Informationen finden Sie unter Zonal Autoshift aktivieren und damit arbeiten.

Um bestimmte zonale Autoshift-Ereignisse zu erfassen, an denen Sie interessiert sind, definieren Sie ereignisspezifische Muster, anhand derer die EventBridge Ereignisse erkannt werden können. Ereignismuster haben dieselbe Struktur wie die Ereignisse, denen sie entsprechen. Das Muster zitiert die Felder, die Sie abgleichen möchten, und liefert die Werte, nach denen Sie suchen.

Ereignisse werden auf bestmögliche Weise ausgegeben. Sie werden unter normalen Betriebsbedingungen nahezu EventBridge in Echtzeit von ARC an übermittelt. Es können jedoch Situationen auftreten, die die Durchführung eines Ereignisses verzögern oder verhindern können.

Informationen darüber, wie EventBridge Regeln mit Ereignismustern funktionieren, finden Sie unter Ereignisse und Ereignismuster in EventBridge.

Überwachen Sie eine zonale Autoshift-Ressource mit EventBridge

Mit können Sie Regeln erstellen EventBridge, die Aktionen definieren, die ergriffen werden sollen, wenn ARC Ereignisse für seine Ressourcen ausgibt. Sie können beispielsweise eine Regel erstellen, die eine E-Mail-Nachricht versendet, wenn ein Übungslauf für zonales Autoshift gestartet wird.

Um ein Ereignismuster einzugeben oder zu kopieren und in die EventBridge Konsole einzufügen, wählen Sie in der Konsole die Option Meine eigene Eingabe aus. Um Ihnen bei der Bestimmung von Ereignismustern zu helfen, die für Sie nützlich sein könnten, enthält dieses Thema Beispiele sowohl für zonale Autoshift-Ereignisabgleichmuster als auch für zonale Autoshift-Ereignisse, die Sie verwenden können.

So erstellen Sie eine Regel für ein Ressourcenereignis

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie AWS-Region die Region aus, in der Sie die Regel erstellen möchten, also die Region, für die Sie sich Ereignisse ansehen möchten.
3. Wählen Sie Create rule (Regel erstellen) aus.
4. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.
5. Behalten Sie für Event Bus den Standardwert default bei.
6. Wählen Sie Weiter aus.
7. Behalten Sie für den Schritt Ereignismuster erstellen für Ereignisquelle den Standardwert AWS Ereignisse bei.

8. Wählen Sie unter Beispielereignis die Option Eigenes Ereignis eingeben aus.
9. Geben Sie für Beispielereignisse ein Ereignismuster ein oder kopieren Sie es und fügen Sie es ein.

Beispiel für zonale Autoshift-Ereignismuster

Ereignismuster haben dieselbe Struktur wie die Ereignisse, denen sie entsprechen. Das Muster zitiert die Felder, die Sie abgleichen möchten, und liefert die Werte, nach denen Sie suchen.

Sie können Ereignismuster aus diesem Abschnitt kopieren und einfügen, um Regeln EventBridge zu erstellen, mit denen Sie zonale Autoshift-Aktionen und -Ressourcen überwachen können.

Wenn Sie Ereignismuster für zonale Autoshift-Ereignisse erstellen, können Sie für Folgendes Folgendes angeben: `detail-type`

- `Autoshift In Progress`
- `Autoshift Completed`
- `Practice Run Started`
- `Practice Run Succeeded`
- `Practice Run Interrupted`
- `Practice Run Failed`
- `FIS Experiment Autoshift In Progress`
- `FIS Experiment Autoshift Completed`
- `FIS Experiment Autoshift Canceled`

Wenn ein Übungslauf unterbrochen wird, finden Sie in dem entsprechenden Feld weitere Informationen zur Ursache der `additionalFailureInfo` Unterbrechung.

Sie können sich dafür entscheiden, alle AWS Autoshifts zu überwachen, indem Sie Autoshift-Observer-Benachrichtigungen aktivieren. Nachdem Sie die Autoshift-Observer-Benachrichtigung aktiviert haben, wählen Sie für den zonalen Autoshift-Detailtyp aus, ob Sie benachrichtigt werden möchten, um Benachrichtigungen zu erhalten. `Autoshift In Progress` Die Schritte zur Aktivierung der Autoshift-Observer-Benachrichtigung finden Sie unter. Zonal Autoshift aktivieren und damit arbeiten

Beispiele finden Sie im Abschnitt Beispiel für zonale Autoshift-Ereignisse.

- Wählen Sie alle Ereignisse aus dem zonalen Autoshift aus, bei denen ein Autoshift gestartet wurde.

  Beachten Sie Folgendes:

  - Wenn Sie die Autoshift-Observer-Benachrichtigung aktiviert haben, gibt ARC alle Autoshift-Ereignisse zurück.
  - Wenn Sie die Autoshift-Observer-Benachrichtigung nicht aktiviert haben, gibt ARC Autoshift-Ereignisse nur zurück, wenn eine Ressource, die Sie für zonales Autoshift konfiguriert haben, in einem Autoshift enthalten ist.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Autoshift In Progress"
    ]
}
```

- Wählen Sie alle Ereignisse aus Zonal Autoshift aus, bei denen ein Übungslauf gestartet wurde.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Started"
    ]
}
```

- Wählen Sie alle Ereignisse aus Zonal Autoshift aus, bei denen ein Übungslauf fehlgeschlagen ist.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Failed"
    ]
}
```

Beispiel für zonale Autoshift-Ereignisse

Dieser Abschnitt enthält Beispielereignisse für zonale Autoshift-Aktionen.

Im Folgenden finden Sie ein Beispielereignis für die `Autoshift In Progress` Aktion, wenn 1) die Autoshift-Observer-Benachrichtigung aktiviert ist und 2) Sie keine Ressource mit zonalem Autoshift konfiguriert haben, die in einer Autoshift enthalten ist:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":"AWS has started an autoshift for an impaired Availability Zone.
 This notification
            is separate from autoshift notifications for resources, if any, that you
 have configured for
            zonal autoshift. For details, see the Developer Guide."
        }
    }
}
```

Im Folgenden finden Sie ein Beispielereignis für die `Autoshift In Progress` Aktion, wenn 1) die Autoshift-Observer-Benachrichtigung deaktiviert ist und 2) Sie eine Ressource mit zonalem Autoshift konfiguriert haben, die in einem Autoshift enthalten ist:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
```

```
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

Das Folgende ist ein Beispielereignis für die Aktion: `Practice Run Interrupted`

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Practice Run Interrupted",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": {
            "additionalFailureInfo": "Practice run interrupted. The blocking alarm
 entered ALARM state."
        },
        "metadata": {
            "awayFrom": "use1-az2"
        }
    }
}
```

Das Folgende ist ein Beispielereignis für die `FIS Experiment Autoshift In Progress` Aktion:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
```

```
    "detail-type": "FIS Experiment Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

Geben Sie eine CloudWatch Protokollgruppe an, die als Ziel verwendet werden soll

Wenn Sie eine EventBridge Regel erstellen, müssen Sie das Ziel angeben, an das Ereignisse gesendet werden, die der Regel entsprechen. Eine Liste der verfügbaren Ziele für EventBridge finden Sie unter In der EventBridge Konsole verfügbare Ziele. Eines der Ziele, die Sie einer EventBridge Regel hinzufügen können, ist eine CloudWatch Amazon-Protokollgruppe. In diesem Abschnitt werden die Anforderungen für das Hinzufügen von CloudWatch Protokollgruppen als Ziele beschrieben und ein Verfahren zum Hinzufügen einer Protokollgruppe beim Erstellen einer Regel beschrieben.

Um eine CloudWatch Protokollgruppe als Ziel hinzuzufügen, können Sie einen der folgenden Schritte ausführen:

- Erstellen Sie eine neue Protokollgruppe
- Wählen Sie eine bestehende Protokollgruppe

Wenn Sie beim Erstellen einer Regel mithilfe der Konsole eine neue Protokollgruppe angeben, EventBridge wird die Protokollgruppe automatisch für Sie erstellt. Stellen Sie sicher, dass die Protokollgruppe, die Sie als Ziel für die EventBridge Regel verwenden, mit beginnt`/aws/events`. Wenn Sie eine bestehende Protokollgruppe auswählen möchten, beachten Sie, dass nur Protokollgruppen, die mit beginnen, als Optionen im Dropdownmenü `/aws/events` angezeigt werden. Weitere Informationen finden Sie unter Neue Protokollgruppe erstellen im CloudWatch Amazon-Benutzerhandbuch.

Wenn Sie eine CloudWatch Protokollgruppe erstellen oder verwenden, um sie mithilfe von CloudWatch Vorgängen außerhalb der Konsole als Ziel zu verwenden, stellen Sie sicher, dass Sie die Berechtigungen korrekt festlegen. Wenn Sie die Konsole verwenden, um einer EventBridge Regel eine Protokollgruppe hinzuzufügen, wird die ressourcenbasierte Richtlinie für die Protokollgruppe automatisch aktualisiert. Wenn Sie jedoch das AWS Command Line Interface oder ein AWS SDK verwenden, um eine Protokollgruppe anzugeben, müssen Sie die ressourcenbasierte Richtlinie für die Protokollgruppe aktualisieren. Die folgende Beispielrichtlinie veranschaulicht die Berechtigungen, die Sie in einer ressourcenbasierten Richtlinie für die Protokollgruppe definieren müssen:

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

Sie können eine ressourcenbasierte Richtlinie für eine Protokollgruppe nicht mithilfe der Konsole konfigurieren. Verwenden Sie den API-Vorgang, um einer ressourcenbasierten Richtlinie die erforderlichen Berechtigungen hinzuzufügen. CloudWatch PutResourcePolicy Anschließend können Sie mit dem describe-resource-policiesCLI-Befehl überprüfen, ob Ihre Richtlinie korrekt angewendet wurde.

Um eine Regel für ein Ressourcenereignis zu erstellen und ein Ziel für die CloudWatch Protokollgruppe anzugeben

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.

2. Wählen Sie AWS-Region die aus, in der Sie die Regel erstellen möchten.
3. Wählen Sie Regel erstellen und geben Sie dann alle Informationen zu dieser Regel ein, z. B. das Ereignismuster oder Details zum Zeitplan.

   Weitere Informationen zum Erstellen von EventBridge Regeln für ARC finden Sie in den Abschnitten weiter oben in diesem Thema.
4. Wählen Sie auf der Seite „Ziel auswählen CloudWatch“ Ihr Ziel aus.
5. Wählen Sie eine CloudWatch Protokollgruppe aus dem Drop-down-Menü aus.

Identity and Access Management für zonales Autoshift

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um ARC-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Inhalt

- Wie funktioniert Zonal Autoshift in ARC mit IAM
- Beispiele für identitätsbasierte Richtlinien für zonales Autoshift
- Verwenden der serviceverknüpften Rolle für zonales Autoshift in ARC
- AWS verwaltete Richtlinien für zonales Autoshift in Amazon Application Recovery Controller (ARC)

Wie funktioniert Zonal Autoshift in ARC mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Zonal Autoshift in Amazon Application Recovery Controller (ARC) zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit Zonal Autoshift verfügbar sind.

IAM-Funktionen, die Sie mit Zonal Autoshift in ARC verwenden können

IAM-Feature	Unterstützung für zonales Autoshift
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja

IAM-Feature	Unterstützung für zonales Autoshift
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für ARC

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 ARC-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien in Amazon Application Recovery Controller (ARC)

Ressourcenbasierte Richtlinien innerhalb von ARC

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.

Politische Maßnahmen für ARC

Unterstützt Richtlinienaktionen: Ja

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

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 keinen passenden API-Vorgang 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 ARC-Aktionen für Zonal Autoshift finden Sie unter Actions defined by Amazon Route 53 Zonal Shift in der Service Authorization Reference.

Richtlinienaktionen in ARC für Zonal Autoshift verwenden vor der Aktion die folgenden Präfixe:

```
arc-zonal-shift
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Zum Beispiel das Folgende:

```
"Action": [
      "arc-zonal-shift:action1",
```

```
      "arc-zonal-shift:action2"
         ]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "arc-zonal-shift:Describe*"
```

Beispiele für identitätsbasierte ARC-Richtlinien für zonales Autoshift finden Sie unter. Beispiele für identitätsbasierte Richtlinien für zonales Autoshift

Richtlinienressourcen für zonales Autoshift in ARC

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 Ressourcentypen und ihrer Aktionen sowie der Aktionen ARNs, die Sie mit dem ARN jeder Ressource angeben können, finden Sie unter dem folgenden Thema in der Service Authorization Reference:

- Von Amazon Route 53 — Zonal Shift definierte Aktionen

Informationen zu den Aktionen und Ressourcen, die Sie mit einem Bedingungsschlüssel verwenden können, finden Sie unter dem folgenden Thema in der Service Authorization Reference:

- Von Amazon Route 53 — Zonal Shift definierte Bedingungsschlüssel

Beispiele für identitätsbasierte ARC-Richtlinien für Zonal Autoshift finden Sie unter. Beispiele für identitätsbasierte Richtlinien für zonales Autoshift

Schlüssel für die Richtlinienbedingung für zonales Autoshift in ARC

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 ARC-Bedingungsschlüssel für zonales Autoshift finden Sie unter den folgenden Themen in der Service Authorization Reference:

- Zustandstasten für Amazon Route 53 Zonal Shift

Informationen zu den Aktionen und Ressourcen, die Sie mit einem Bedingungsschlüssel verwenden können, finden Sie in den folgenden Themen in der Service Authorization Reference:

- Von Amazon Route 53 Zonal Shift definierte Aktionen

Beispiele für identitätsbasierte ARC-Richtlinien für Zonal Autoshift finden Sie unter. Beispiele für identitätsbasierte Richtlinien für zonales Autoshift

Zugriffskontrolllisten () in ARC ACLs

Unterstützt ACLs: Nein

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

Attributbasierte Zugriffskontrolle (ABAC) mit ARC

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt 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 Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

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

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Zonal Autoshift in ARC beinhaltet die folgende teilweise Unterstützung für ABAC:

- Zonal Autoshift unterstützt ABAC für verwaltete Ressourcen, die in ARC für Zonal Shift registriert sind. Weitere Informationen zu den verwalteten Ressourcen von ABAC for Network Load Balancer und Application Load Balancer finden Sie unter ABAC with Elastic Load Balancing im Elastic Load Balancing User Guide.

Temporäre Anmeldeinformationen mit ARC verwenden

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 von einer Benutzerrolle zu einer IAM-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.

Serviceübergreifende Prinzipalberechtigungen für ARC

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie eine IAM-Entität (Benutzer oder Rolle) verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Richtlinien erteilen einem Prinzipal-Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen.

Informationen darüber, ob für eine Aktion zusätzliche abhängige Aktionen in einer Richtlinie erforderlich sind, finden Sie unter dem folgenden Thema in der Service Authorization Reference:

- Amazon Route 53 Zonenverschiebung

Servicerollen für ARC

Unterstützt Servicerollen: Nein

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.

Dienstbezogene Rollen für ARC

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte 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. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen ARC-Rollen finden Sie unter. Verwenden der serviceverknüpften Rolle für zonales Autoshift in ARC

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für zonales Autoshift

Standardmäßig sind Benutzer und Rollen nicht berechtigt, ARC-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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von ARC definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Application Recovery Controller (ARC) in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Beispiel: Zonaler Autoshift-Konsolenzugriff
- Beispiele: ARC-API-Aktionen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand ARC-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 Richtlinienvalidierung mit 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 Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Beispiel: Zonaler Autoshift-Konsolenzugriff

Um auf die Amazon Application Recovery Controller (ARC) -Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den ARC-Ressourcen in Ihrem aufzulisten und anzuzeigen 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 API 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 einige Aufgaben ausführen zu können, müssen Benutzer über die Berechtigung verfügen, die dienstbezogene Rolle zu erstellen, die mit Zonal Autoshift in ARC verknüpft ist. Weitere Informationen hierzu finden Sie unter Verwenden der serviceverknüpften Rolle für zonales Autoshift in ARC.

Um Benutzern vollen Zugriff auf die Nutzung von Zonal Autoshift in der zu gewähren AWS Management Console, fügen Sie dem Benutzer eine Richtlinie wie die folgende hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift",
                   "arc-zonal-shift:CreatePracticeRunConfiguration",
                   "arc-zonal-shift:DeletePracticeRunConfiguration",
                   "arc-zonal-shift:ListAutoshifts",
                   "arc-zonal-shift:UpdatePracticeRunConfiguration",
                   "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:DescribeAlarms",
            "Resource": "*"
        }
    ]
}
```

Beispiele: ARC-API-Aktionen

Sie können eine Richtlinie verwenden, um sicherzustellen, dass ein Benutzer ARC-API-Aktionen für zonales Autoshift verwenden kann, um zonales Autoshift so zu konfigurieren, dass AWS der Datenverkehr der Anwendungsressourcen von einer Availability Zone in Ihrem Namen auf Healthy AZs in the umgeleitet wird, um die AWS-Region Zeit bis zur Wiederherstellung bei Ereignissen zu

verkürzen. Um diese Berechtigungen bereitzustellen, fügen Sie eine Richtlinie hinzu, die den API-Vorgängen entspricht, mit denen der Benutzer arbeiten muss, wie unten beschrieben.

Um einige Aufgaben ausführen zu können, müssen Benutzer über Berechtigungen für die dienstbezogene Rolle verfügen, die mit ARC verknüpft ist. Die zum Erstellen der serviceverknüpften Rolle erforderlichen Berechtigungen sind in der folgenden Beispielrichtlinie enthalten. Weitere Informationen hierzu finden Sie unter Verwenden der serviceverknüpften Rolle für zonales Autoshift in ARC.

Um mit API-Operationen für zonales Autoshift zu arbeiten, fügen Sie dem Benutzer eine Richtlinie wie die folgende hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift",
                   "arc-zonal-shift:CreatePracticeRunConfiguration",
                   "arc-zonal-shift:DeletePracticeRunConfiguration",
                   "arc-zonal-shift:ListAutoshifts",
                   "arc-zonal-shift:UpdatePracticeRunConfiguration",
                   "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
            "Resource": "*"
        },
        {
            "Effect" : "Allow",
            "Action" : [
                    "cloudwatch:DescribeAlarms",
                    "health:DescribeEvents"
            ],
            "Resource" : "*"
        },
        {
            "Effect" : "Allow",
            "Action" : [
```

```
                    "arc-zonal-shift:CancelZonalShift",
                    "arc-zonal-shift:GetManagedResource",
                    "arc-zonal-shift:StartZonalShift",
                    "arc-zonal-shift:UpdateZonalShift"
            ],
            "Resource" : "*"
        }
    ]
}
```

Verwenden der serviceverknüpften Rolle für zonales Autoshift in ARC

Zonal Autoshift in Amazon Application Recovery Controller verwendet eine AWS Identity and Access Management (IAM) -Serviceverknüpfte Rolle. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit einem Service verknüpft ist — in diesem Fall ARC. Die dienstbezogene Rolle ist von ARC vordefiniert und umfasst alle Berechtigungen, die der Dienst benötigt, um in Ihrem Namen andere AWS Dienste für bestimmte Zwecke aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von ARC, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. ARC definiert die Berechtigungen für die dienstbezogene Rolle, und sofern nicht anders definiert, kann nur ARC ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen juristischen Stelle von IAM zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre zonalen ARC-Autoshift-Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Dienstverknüpfte Rolle nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen für dienstverknüpfte Rollen AWSService RoleForZonalAutoshiftPracticeRun

ARC verwendet die benannte serviceverknüpfte Rolle AWSServiceRoleForZonalAutoshiftPracticeRunfür folgende Zwecke:

- Überwachen Sie von Kunden bereitgestellte CloudWatch Amazon-Alarme und AWS Health Dashboard Kundenereignisse für Übungsläufe

- Übungsläufe verwalten (Zonenverschiebungen üben)

In diesem Abschnitt werden die Berechtigungen für die dienstverknüpfte Rolle sowie Informationen zum Erstellen, Bearbeiten und Löschen der Rolle beschrieben.

Berechtigungen für dienstverknüpfte Rollen für AWSService RoleForZonalAutoshiftPracticeRun

Diese dienstbezogene Rolle verwendet die verwaltete RichtlinieAWSZonalAutoshiftPracticeRunSLRPolicy.

Die serviceverknüpfte Rolle AWSServiceRoleForZonalAutoshiftPracticeRun vertraut darauf, dass der folgende Service die Rolle annimmt:

- `practice-run.arc-zonal-shift.amazonaws.com`

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSZonalAutoshiftPracticeRunSLRPolicy in der Referenz zu von AWS verwalteten Richtlinien.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Die AWSServiceRoleForZonalAutoshiftPracticeRundienstbezogene Rolle für ARC wird erstellt

Sie müssen die serviceverknüpfte Rolle AWSServiceRoleForZonalAutoshiftPracticeRun nicht manuell erstellen. Wenn Sie die Konfiguration für den ersten Übungslauf im AWS Management Console, dem oder einem AWS SDK erstellen AWS CLI, erstellt ARC die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie die Konfiguration für den ersten Übungslauf erstellen, erstellt ARC die serviceverknüpfte Rolle erneut für Sie.

Die AWSServiceRoleForZonalAutoshiftPracticeRunserviceverknüpfte Rolle für ARC bearbeiten

ARC erlaubt es Ihnen nicht, die AWSServiceRoleForZonalAutoshiftPracticeRunserviceverknüpfte Rolle zu bearbeiten. Nachdem Sie die dienstverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da andere Entitäten möglicherweise darauf verweisen. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der AWSServiceRoleForZonalAutoshiftPracticeRundienstbezogenen Rolle für ARC

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für eine dienstverknüpfte Rolle bereinigen, bevor Sie sie manuell löschen können.

Nachdem Sie Autoshift deaktiviert haben, können Sie die AWSServiceRoleForZonalAutoshiftPracticeRundienstverknüpfte Rolle löschen. Weitere Informationen zur Autoshift-Funktion finden Sie unter. Zonenverschiebung in ARC

> **Note**
>
> Wenn der ARC-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen der Servicerolle möglicherweise fehl. Warten Sie in diesem Fall einige Minuten und versuchen Sie erneut, die Rolle zu löschen.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSService RoleForZonalAutoshiftPracticeRun serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Aktualisierungen der dienstverknüpften ARC-Rolle für zonales Autoshift

Aktualisierungen der AWS verwalteten Richtlinien für die mit dem ARC-Dienst verknüpften Rollen finden Sie in der Tabelle mit Aktualisierungen AWS verwalteter Richtlinien für ARC. Sie können auch automatische RSS-Benachrichtigungen auf der Seite mit dem Verlauf der ARC-Dokumente abonnieren.

AWS verwaltete Richtlinien für zonales Autoshift in Amazon Application Recovery Controller (ARC)

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, 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 vom Kunden verwaltete 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.

AWS verwaltete Richtlinie: AWSZonal AutoshiftPracticeRun SLRPolicy

Sie können `AWSZonalAutoshiftPracticeRunSLRPolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer servicebezogenen Rolle verknüpft, die es Amazon Application Recovery Controller (ARC) ermöglicht, für zonales Autoshift Folgendes zu tun:

- Überwachen Sie von Kunden bereitgestellte CloudWatch Amazon-Alarme und AWS Health Dashboard Kundenereignisse für Übungsläufe
- Übungsläufe verwalten (Zonenverschiebungen üben)

Weitere Informationen finden Sie unter Verwenden der serviceverknüpften Rolle für zonales Autoshift in ARC.

Aktualisierungen für AWS verwaltete Richtlinien für zonales Autoshift

Einzelheiten zu den Aktualisierungen der AWS verwalteten Richtlinien für zonal Autoshift in ARC seit Beginn der Erfassung dieser Änderungen durch diesen Dienst finden Sie unter. Aktualisierungen der AWS verwalteten Richtlinien für Amazon Application Recovery Controller (ARC) Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite ARC-Dokumentenverlauf.

Verwenden Sie die Routingsteuerung, um Anwendungen mit mehreren Regionen in ARC wiederherzustellen

In diesem Abschnitt wird erklärt, wie Sie die Routing-Steuerungsfunktion in Amazon Application Recovery Controller (ARC) nutzen können, um Unterbrechungen zu minimieren und die Kontinuität für Ihre Benutzer zu gewährleisten, wenn Sie eine AWS Anwendung in mehreren bereitstellen AWS-Regionen.

Sie können sich auch mit dem Readiness Check vertraut machen, einer Funktion in ARC, mit der Sie herausfinden können, ob Ihre Anwendungen und Ressourcen für die Wiederherstellung vorbereitet sind.

In den Themen in diesem Abschnitt werden die Funktionen zur Routingsteuerung und zur Prüfung der Bereitschaft beschrieben, wie sie eingerichtet und verwendet werden.

Themen

- Routing-Steuerung in ARC
- Bereitschaftsprüfung in ARC

Routing-Steuerung in ARC

Um den Datenverkehr an mehrere Anwendungsreplikate weiterzuleiten AWS-Regionen, können Sie Routing-Steuerelemente in Amazon Application Recovery Controller (ARC) verwenden, die in eine bestimmte Art von Zustandsprüfung in Amazon Route 53 integriert sind. Routing-Steuerelemente sind einfache Ein- und Ausschalter, mit denen Sie Ihren Client-Verkehr von einem regionalen Replikat auf ein anderes umschalten können. Die Umleitung des Datenverkehrs erfolgt durch Zustandsprüfungen der Routing-Kontrolle, die mit Amazon Route 53-DNS-Einträgen eingerichtet werden. Zum Beispiel DNS-Failover-Einträge, die mit Domainnamen verknüpft sind, die Ihren Anwendungsreplikaten in jeder Region zugeordnet sind.

In diesem Abschnitt wird erklärt, wie die Routingsteuerung funktioniert, wie Routingsteuerungskomponenten eingerichtet werden und wie sie verwendet werden, um den Datenverkehr für ein Failover umzuleiten.

Die Routing-Steuerungskomponenten in ARC sind: Cluster, Bedienfelder, Routingsteuerungen und Zustandsprüfungen der Routing-Steuerung. Alle Routing-Steuerelemente sind in Bedienfeldern

gruppiert. Sie können sie auf dem Standard-Bedienfeld gruppieren, das ARC für Ihren Cluster erstellt, oder Sie können Ihre eigenen benutzerdefinierten Bedienfelder erstellen. Sie müssen einen Cluster erstellen, bevor Sie ein Control Panel oder eine Routing-Steuerung erstellen können. Jeder Cluster in ARC ist eine Datenebene mit fünf AWS-Regionen Endpunkten.

Nachdem Sie Routingkontrollen und Integritätsprüfungen für die Routingsteuerung erstellt haben, können Sie Sicherheitsregeln für die Routingsteuerung erstellen, um unbeabsichtigte Nebenwirkungen der Wiederherstellungsautomatisierung zu vermeiden. Sie können den Status der Routingsteuerung aktualisieren, um den Verkehr einzeln oder stapelweise umzuleiten, indem Sie die API-Aktionen AWS CLI oder (empfohlen) oder die verwenden. AWS Management Console

In diesem Abschnitt wird erklärt, wie Routingkontrollen funktionieren und wie Sie sie erstellen und verwenden, um den Datenverkehr für Ihre Anwendung umzuleiten.

> **Important**
>
> Weitere Informationen zur Vorbereitung der Verwendung von ARC zur Umleitung von Datenverkehr als Teil eines Failoverplans für Ihre Anwendung in einem Notfallszenario finden Sie unter. Bewährte Methoden für die Routingsteuerung in ARC

Informationen zur Routingsteuerung

Die Routingsteuerung leitet den Datenverkehr mithilfe von Zustandsprüfungen in Amazon Route 53 um, die mit DNS-Einträgen konfiguriert sind, die der obersten Ressource der Zellen in Ihrer Wiederherstellungsgruppe zugeordnet sind, z. B. einem Elastic Load Balancing Load Balancer. Sie können den Verkehr von einer Zelle zu einer anderen umleiten, indem Sie beispielsweise einen Routing-Kontrollstatus auf aktualisieren `Off` (um den Datenfluss zu einer Zelle zu stoppen) und einen anderen Routing-Kontrollstatus auf `On` (um den Datenfluss zu einer anderen zu starten) aktualisieren. Der Prozess, der den Verkehrsfluss verändert, ist die mit der Routingsteuerung verknüpfte Zustandsprüfung von Route 53, nachdem ARC sie aktualisiert hat, um sie je nach dem entsprechenden Status der Routingsteuerung als fehlerfrei oder fehlerhaft festzulegen.

Routingkontrollen unterstützen Failover für alle AWS Dienste, die über einen DNS-Endpunkt verfügen. Sie können den Status der Routing-Steuerung so aktualisieren, dass der Datenverkehr für die Notfallwiederherstellung, wenn Sie Latenzabfälle bei Ihrer Anwendung oder andere Probleme feststellen, ein Failover durchführt.

Sie können auch Sicherheitsregeln für die Routingsteuerung konfigurieren, um sicherzustellen, dass die Umleitung des Datenverkehrs mithilfe von Routingkontrollen die Verfügbarkeit nicht beeinträchtigt. Weitere Informationen finden Sie unter Sicherheitsregeln für die Routingsteuerung erstellen .

Es ist wichtig zu beachten, dass Routingkontrollen selbst keine Integritätsprüfungen sind, mit denen der zugrunde liegende Zustand der Endgeräte überwacht wird. Im Gegensatz zu einer Route 53-Zustandsprüfung überwacht eine Routingsteuerung beispielsweise keine Antwortzeiten oder TCP-Verbindungszeiten. Eine Routingsteuerung ist ein einfacher Ein-/Ausschalter, der eine Zustandsprüfung steuert. In der Regel ändern Sie den Status, um den Datenverkehr umzuleiten, und durch diese Statusänderung wird der Datenverkehr für einen gesamten Anwendungsstapel an einen bestimmten Endpunkt verschoben oder das Routing an den gesamten Anwendungsstapel verhindert. Wenn Sie beispielsweise in einem einfachen Szenario den Status einer Routingsteuerung von `On` zu ändern`Off`, wird dadurch eine Route 53-Zustandsprüfung aktualisiert, die Sie mit einem DNS-Failover-Datensatz verknüpft haben, um den Datenverkehr von einem Endpunkt abzuleiten.

Wie verwendet man die Routingsteuerung

Um den Status einer Routingsteuerung zu aktualisieren, sodass Sie den Verkehr umleiten können, müssen Sie eine Verbindung zu einem Ihrer Cluster-Endpunkte in ARC herstellen. Wenn der Endpunkt, zu dem Sie eine Verbindung herstellen möchten, nicht verfügbar ist, versuchen Sie, den Status mit einem anderen Cluster-Endpunkt zu ändern. Bei der Änderung des Status der Routingsteuerung sollten Sie darauf vorbereitet sein, jeden Endpunkt abwechselnd zu testen, da die Cluster-Endpunkte für regelmäßige Wartungs- und Aktualisierungsarbeiten zyklisch den Status „Verfügbar“ und „Nicht verfügbar“ durchlaufen.

Wenn Sie Routingkontrollen erstellen, konfigurieren Sie Ihre DNS-Einträge so, dass Zustandsprüfungen der Routingsteuerung den Route 53-DNS-Namen zugeordnet werden, vor denen jedes Anwendungsreplikat steht. Um beispielsweise Datenverkehrs-Failover zwischen zwei Load Balancern, einem in jeder von zwei Regionen, zu kontrollieren, erstellen Sie zwei Zustandsprüfungen für die Routingsteuerung und verknüpfen sie mit zwei DNS-Einträgen, z. B. Alias-Datensätzen mit Failover-Routing-Richtlinien, mit den Domänennamen der jeweiligen Load Balancer.

Sie können auch komplexere Verkehrs-Failover-Szenarien einrichten, indem Sie die ARC-Routingsteuerung zusammen mit Route 53-Zustandsprüfungen und DNS-Datensätzen verwenden und DNS-Datensätze mit gewichteten Routing-Richtlinien verwenden. Ein detailliertes Beispiel finden Sie im Abschnitt zum Failover von Benutzerdatenverkehr im folgenden AWS Blogbeitrag: Hochbelastbare Anwendungen mit Amazon Application Recovery Controller (ARC) erstellen, Teil 2: Multi-Region-Stack

Wenn Sie einen Failover für eine AWS-Region Routing Control starten, werden Sie aufgrund der mit dem Datenfluss verbundenen Schritte möglicherweise nicht sofort feststellen, dass der Verkehr die Region verlässt. Je nach Verhalten des Clients und der Wiederverwendung von Verbindungen kann es auch eine kurze Zeit dauern, bis bestehende, in Bearbeitung befindliche Verbindungen in der Region abgeschlossen sind. Abhängig von Ihren DNS-Einstellungen und anderen Faktoren können bestehende Verbindungen in nur wenigen Minuten abgeschlossen werden oder länger dauern. Weitere Informationen finden Sie unter Sicherstellen, dass Verkehrsverlagerungen schnell abgeschlossen werden.

Vorteile der Routingsteuerung

Eine Routingsteuerung in ARC bietet mehrere Vorteile gegenüber der Umleitung von Datenverkehr mit herkömmlichen Zustandsprüfungen. Zum Beispiel:

- Eine Routingsteuerung bietet Ihnen die Möglichkeit, ein Failover für einen gesamten Anwendungsstapel durchzuführen. Dies steht im Gegensatz zu einem Failover einzelner Komponenten eines Stacks, wie dies Amazon EC2 Amazon-Instances auf der Grundlage von Zustandsprüfungen auf Ressourcenebene der Fall ist.
- Eine Routing-Steuerung bietet Ihnen eine sichere, einfache manuelle Übersteuerung, mit der Sie den Datenverkehr für Wartungsarbeiten oder für die Wiederherstellung nach Ausfällen verwenden können, wenn interne Monitore kein Problem erkennen.
- Sie können eine Routingsteuerung zusammen mit Sicherheitsregeln verwenden, um häufige Nebenwirkungen zu vermeiden, die bei einer vollautomatischen Automatisierung auf der Grundlage von Integritätsprüfungen auftreten können, z. B. ein Failover auf eine Standby-Infrastruktur, die nicht auf einen Failover vorbereitet ist.

Hier ist ein Beispiel für die Integration von Routingkontrollen in Ihre Failover-Strategie, um die Widerstandsfähigkeit und Verfügbarkeit Ihrer Anwendungen in zu verbessern. AWS

Sie können hochverfügbare AWS Anwendungen unterstützen, AWS indem Sie mehrere (in der Regel drei) redundante Replikate in verschiedenen Regionen ausführen. Anschließend können Sie Amazon Route 53 Routing Control verwenden, um den Verkehr an das entsprechende Replikat weiterzuleiten.

Sie können beispielsweise ein Anwendungsreplikat so einrichten, dass es aktiv ist und den Anwendungsdatenverkehr bedient, während es sich bei einem anderen um ein Standby-Replikat handelt. Wenn Ihr aktives Replikat ausfällt, können Sie den Benutzerverkehr dorthin umleiten, um die Verfügbarkeit Ihrer Anwendung wiederherzustellen. Sie sollten anhand der Informationen aus Ihren

Überwachungs- und Integritätsprüfungssystemen entscheiden, ob Sie ein Failaway oder ein Replikat verwenden möchten.

Wenn Sie schnellere Wiederherstellungen ermöglichen möchten, ist eine Active-Active-Implementierung eine weitere Option, die Sie für Ihre Architektur wählen können. Bei diesem Ansatz sind Ihre Replikate gleichzeitig aktiv. Das bedeutet, dass Sie sich nach Ausfällen erholen können, indem Sie Benutzer von einem beeinträchtigten Anwendungsreplikat wegbewegen, indem Sie den Datenverkehr einfach auf ein anderes aktives Replikat umleiten.

AWS Regionale Verfügbarkeit für die Routing-Steuerung

Detaillierte Informationen zu regionalen Support- und Service-Endpunkten für Amazon Application Recovery Controller (ARC) finden Sie unter Amazon Application Recovery Controller (ARC) - Endpunkte und Kontingente in der Amazon Web Services General Reference.

> **Note**
>
> Die Routing-Steuerung in Amazon Application Recovery Controller (ARC) ist eine globale Funktion. In den regionalen AWS CLI ARC-Befehlen müssen Sie jedoch die Region USA West (Oregon`--region us-west-2`) angeben (geben Sie den Parameter an). Das heißt, wenn Sie Ressourcen wie Cluster, Bedienfelder oder Routingsteuerungen erstellen.

Bei einer ARC-Routingsteuerung handelt es sich um einen Ein-/Ausschalter, der den Status einer ARC-Zustandsprüfung ändert. Diese kann dann einem DNS-Eintrag zugeordnet werden, der den Datenverkehr beispielsweise von einem primären Replikat zu einem Standby-Bereitstellungsreplikat umleitet.

Wenn eine Anwendung ausfällt oder ein Latenzproblem auftritt, können Sie den Status der Routing-Steuerung aktualisieren, um den Datenverkehr von Ihrem primären Replikat beispielsweise auf ein Standby-Replikat zu verlagern. Durch die Verwendung der äußerst zuverlässigen ARC-Datenebenen-API-Operationen zur Durchführung von Routingsteuerungsabfragen und Statusaktualisierungen der Routingsteuerung können Sie sich beim Failover in Notfallwiederherstellungsszenarien auf ARC verlassen. Weitere Informationen finden Sie unter Status der Routingsteuerung mithilfe der ARC-API abrufen und aktualisieren (empfohlen).

ARC verwaltet die Routing-Kontrollstatus in einem Cluster, der aus fünf redundanten regionalen Endpunkten besteht. ARC verbreitet Statusänderungen der Routing-Steuerung im gesamten Cluster,

der sich in einer EC2 Amazon-Flotte befindet, um ein Quorum für fünf AWS Regionen zu erreichen. Wenn Sie nach der Propagierung ARC mithilfe der API und der äußerst zuverlässigen Datenebene nach einem Status der Routing-Kontrolle abfragen, wird die Konsensansicht zurückgegeben.

Sie können mit jedem der fünf Cluster-Endpunkte interagieren, um den Status einer Routing-Steuerung zu aktualisieren, z. B. von. `0ff` `0n` Anschließend verteilt ARC das Update auf die fünf Regionen des Clusters.

Die Datenkonsistenz zwischen allen fünf Cluster-Endpunkten wird im Durchschnitt innerhalb von 5 Sekunden und nach maximal 15 Sekunden erreicht.

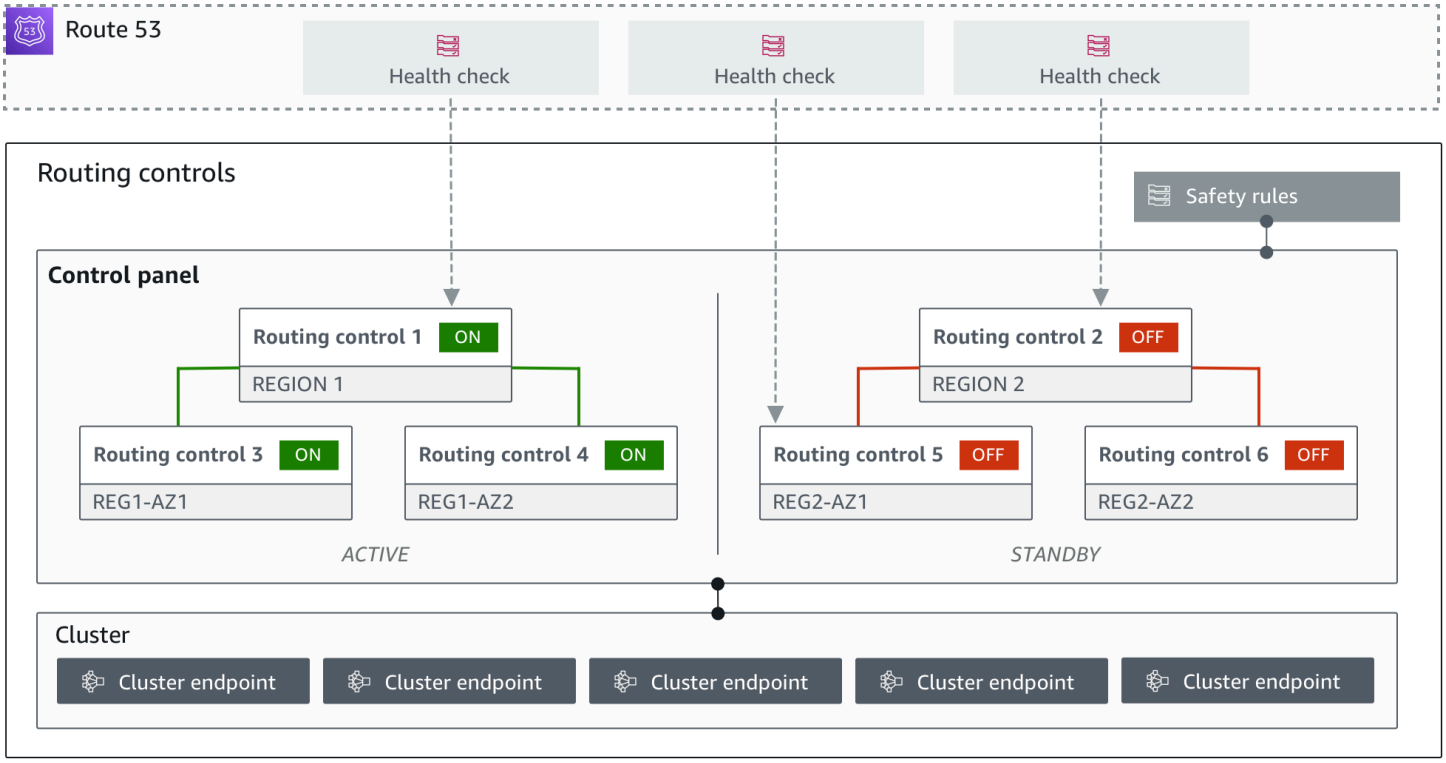
ARC bietet mit seiner Datenebene extreme Zuverlässigkeit, sodass Sie für Ihre Anwendung manuell ein zellenübergreifendes Failover durchführen können. ARC stellt sicher, dass Sie jederzeit auf mindestens drei der fünf Cluster-Endpunkte zugreifen können, um Statusänderungen der Routing-Steuerung vorzunehmen. Beachten Sie, dass es sich bei jedem ARC-Cluster um einen Single-Tenant-Cluster handelt, um sicherzustellen, dass Sie nicht von „störenden Nachbarn“ betroffen sind, die Ihre Zugriffsmuster verlangsamen könnten.

Wenn Sie Änderungen an den Status der Routing-Steuerung vornehmen, verlassen Sie sich auf die folgenden drei Kriterien, bei denen es sehr unwahrscheinlich ist, dass sie fehlschlagen:

- Mindestens drei Ihrer fünf Endpunkte sind verfügbar und nehmen am Quorum teil.
- Sie verfügen über funktionierende IAM-Anmeldeinformationen und können sich an einem funktionierenden regionalen Cluster-Endpunkt authentifizieren.
- Die Route 53-Datenebene ist fehlerfrei (diese Datenebene wurde so konzipiert, dass sie eine SLA mit 100-prozentiger Verfügbarkeit erfüllt).

Komponenten zur Routing-Steuerung

Das folgende Diagramm zeigt ein Beispiel für Komponenten, die die Routing-Steuerungsfunktion in ARC unterstützen. Mit den hier gezeigten Routing-Steuerelementen (gruppiert in einem Control Panel) können Sie den Verkehr zu zwei Availability Zones in jeder der beiden Regionen verwalten. Wenn Sie den Status der Routing-Kontrolle aktualisieren, ändert ARC die Zustandsprüfungen in Amazon Route 53, wodurch der DNS-Verkehr zu verschiedenen Zellen umgeleitet wird. Sicherheitsregeln, die Sie für Routingkontrollen konfigurieren, tragen dazu bei, Fail-Open-Szenarien und andere unbeabsichtigte Folgen zu vermeiden.



Im Folgenden sind die Komponenten der Routing-Steuerungsfunktion in ARC aufgeführt.

Cluster

Ein Cluster besteht aus fünf redundanten regionalen Endpunkten, für die Sie API-Aufrufe initiieren, um den Status der Routing-Steuerung zu aktualisieren oder abzurufen. Ein Cluster umfasst ein Standard-Control Panel, und Sie können mehrere Control Panels und Routing-Steuerelemente auf einem Cluster hosten.

Routing-Steuerelemente

Eine Routingsteuerung ist ein einfacher Ein-/Ausschalter, der auf einem Cluster gehostet wird und mit dem Sie das Routing des Client-Datenverkehrs in und aus Zellen steuern. Wenn Sie eine Routingsteuerung erstellen, fügen Sie in Route 53 eine ARC-Integritätsprüfung hinzu. Auf diese Weise können Sie den Datenverkehr umleiten (mithilfe der Integritätsprüfungen, die mit DNS-Einträgen für Ihre Anwendungen konfiguriert sind), wenn Sie den Status der Routingsteuerung in ARC aktualisieren.

Zustandsprüfung der Routingsteuerung

Die Routingkontrollen sind in Route 53 in die Integritätsprüfungen integriert. Die Integritätsprüfungen sind mit DNS-Einträgen verknüpft, die für jedes Anwendungsreplikat verwendet werden, z. B. Failover-Datensätze. Wenn Sie den Status der Routingsteuerung ändern,

aktualisiert ARC die entsprechenden Integritätsprüfungen, die den Datenverkehr umleiten, z. B. um ein Failover auf Ihr Standby-Replikat durchzuführen.

Systemsteuerung

Ein Bedienfeld gruppiert eine Reihe verwandter Routing-Steuerelemente. Sie können einem Control Panel mehrere Routing-Steuerelemente zuordnen und anschließend Sicherheitsregeln für das Control Panel erstellen, um sicherzustellen, dass die von Ihnen vorgenommenen Aktualisierungen der Verkehrsumleitung sicher sind. Sie können beispielsweise eine Routingsteuerung für jeden Ihrer Load Balancer in jeder Availability Zone konfigurieren und sie dann im selben Control Panel gruppieren. Anschließend können Sie eine Sicherheitsregel (eine „Assertion-Regel“) hinzufügen, die sicherstellt, dass mindestens eine Zone (dargestellt durch eine Routing-Steuerung) gleichzeitig aktiv ist, um unbeabsichtigte „Fail-Open“ -Szenarien zu vermeiden.

Standard-Systemsteuerung

Wenn Sie einen Cluster erstellen, erstellt ARC ein Standard-Control-Panel. Standardmäßig werden alle Routing-Steuerelemente, die Sie auf dem Cluster erstellen, dem Standard-Control-Panel hinzugefügt. Sie können auch Ihre eigenen Bedienfelder erstellen, um verwandte Routing-Steuerelemente zu gruppieren.

Sicherheitsregel

Sicherheitsregeln sind Regeln, die Sie zur Routing-Steuerung hinzufügen, um sicherzustellen, dass Wiederherstellungsaktionen die Verfügbarkeit Ihrer Anwendung nicht versehentlich beeinträchtigen. Sie können beispielsweise eine Sicherheitsregel erstellen, die eine Routingsteuerung erstellt, die als allgemeiner Ein-/Ausschalter fungiert, sodass Sie eine Reihe anderer Routingsteuerungen aktivieren oder deaktivieren können.

Endpunkt (Cluster-Endpunkt)

Jeder Cluster in ARC hat fünf regionale Endpunkte, die Sie zum Einstellen und Abrufen von Routingsteuerungsstatus verwenden können. Bei Ihrem Verfahren für den Zugriff auf die Endgeräte sollte davon ausgegangen werden, dass ARC die Endpunkte zur Wartung regelmäßig hoch- und herunterfährt. Sie sollten also jeden Endpunkt nacheinander testen, bis Sie eine Verbindung zu einem herstellen. Sie greifen auf die Endgeräte zu, um den aktuellen Status der Routing-Steuerung (Ein oder Aus) abzurufen und Failover für Ihre Anwendungen auszulösen, indem Sie den Status der Routing-Steuerung ändern.

Daten- und Steuerungsebenen für die Routing-Steuerung

Denken Sie bei der Planung von Failover und Disaster Recovery darüber nach, wie robust Ihre Failover-Mechanismen sind. Es wird empfohlen, sicherzustellen, dass die Mechanismen, auf die Sie beim Failover angewiesen sind, hochverfügbar sind, sodass Sie sie bei Bedarf in einem Notfallszenario verwenden können. In der Regel sollten Sie, wann immer möglich, Datenebenenfunktionen für Ihre Mechanismen verwenden, um die größtmögliche Zuverlässigkeit und Fehlertoleranz zu gewährleisten. Vor diesem Hintergrund ist es wichtig zu verstehen, wie die Funktionalität eines Dienstes zwischen Steuerungsebenen und Datenebenen aufgeteilt ist und wann Sie sich darauf verlassen können, dass die Datenebene eines Dienstes extrem zuverlässig ist.

Wie bei den meisten AWS Diensten wird die Funktionalität für die Routing-Steuerung durch Steuerungsebenen und Datenebenen unterstützt. Beide sind zwar auf Zuverlässigkeit ausgelegt, eine Steuerungsebene ist jedoch für die Datenkonsistenz optimiert, während eine Datenebene für die Verfügbarkeit optimiert ist. Eine Datenebene ist auf Ausfallsicherheit ausgelegt, sodass sie die Verfügbarkeit auch bei Störungen aufrechterhalten kann, wenn eine Kontrollebene möglicherweise nicht verfügbar ist.

Im Allgemeinen ermöglicht Ihnen eine Kontrollebene grundlegende Verwaltungsfunktionen wie das Erstellen, Aktualisieren und Löschen von Ressourcen im Service. Eine Datenebene stellt die Kernfunktionalität eines Dienstes bereit. Aus diesem Grund empfehlen wir, Datenebenenoperationen zu verwenden, wenn Verfügbarkeit wichtig ist, z. B. wenn Sie den Datenverkehr während eines Ausfalls auf ein Standby-Replikat umleiten müssen.

Bei der Routingsteuerung sind die Steuerungsebenen und Datenebenen wie folgt aufgeteilt:

- Die Steuerungsebenen-API für die Routingsteuerung ist die Recovery Control Configuration API, die in der Region USA West (Oregon) (us-west-2) unterstützt wird. Sie verwenden diese API-Operationen oder die, AWS Management Console um Cluster, Control Panels und Routing-Steuerelemente zu erstellen oder zu löschen, um sich auf ein Disaster Recovery-Ereignis vorzubereiten, bei dem Sie möglicherweise den Datenverkehr für Ihre Anwendung umleiten müssen. Die Steuerungsebene für die Konfiguration der Routing-Steuerung ist nicht hochverfügbar.
- Die Datenebene der Routing-Steuerung ist ein dedizierter Cluster, der sich über fünf geografisch isolierte Regionen erstreckt AWS . Jeder Kunde erstellt mithilfe der Routing-Steuerebene einen oder mehrere Cluster. Der Cluster hostet Bedienfelder und Routingsteuerungen. Anschließend verwenden Sie die Routing Control (Recovery Cluster) API, um den Status der Routingsteuerung abzurufen, aufzulisten und zu aktualisieren, wenn Sie den Datenverkehr für Ihre Anwendung umleiten möchten. Die Datenebene der Routingsteuerung IST hochverfügbar.

Da die Datenebene der Routingsteuerung hochverfügbar ist, empfehlen wir Ihnen, die für API-Aufrufe zu verwenden, AWS Command Line Interface um mit den Status der Routingsteuerung zu arbeiten, wenn Sie zur Wiederherstellung nach einem Ereignis ein Failover durchführen möchten. Weitere Informationen zu den wichtigsten Überlegungen bei der Vorbereitung und beim Abschluss eines Wiederherstellungsvorgangs mit Routingsteuerung finden Sie unterBewährte Methoden für die Routingsteuerung in ARC.

Weitere Informationen zu Datenebenen, Kontrollebenen und dazu, wie Services AWS entwickelt werden, um Hochverfügbarkeitsziele zu erreichen, finden Sie im paper Statische Stabilität mithilfe von Availability Zones in der Amazon Builders' Library.

Tagging für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)

Tags sind Wörter oder Ausdrücke (Metadaten), die Sie verwenden, um Ihre AWS Ressourcen zu identifizieren und zu organisieren. Sie können jeder Ressource mehrere Tags hinzufügen, und jedes Tag enthält einen Schlüssel und einen Wert, den Sie festlegen. Der Schlüssel könnte beispielsweise die Umwelt und der Wert die Produktion sein. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags durchsuchen und filtern.

Sie können die folgenden Ressourcen in der Routing-Steuerung in ARC taggen:

- Cluster
- Bedienfelder
- Sicherheitsregeln

Tagging in ARC ist nur über die API verfügbar, z. B. mit der AWS CLI.

Im Folgenden finden Sie Beispiele für das Tagging in der Routing-Steuerung mithilfe von. AWS CLI

```
aws route53-recovery-control-config --region us-west-2 create-cluster --
cluster-name example1-cluster --tags Region=PDX,Stage=Prod
```

```
aws route53-recovery-control-config --region us-west-2 create-control-panel
--control-panel-name example1-control-panel --cluster-arn arn:aws:route53-
recovery-control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
--tags Region=PDX,Stage=Prod
```

Weitere Informationen finden Sie TagResourceim Referenzhandbuch zur Recovery Control Configuration API für Amazon Application Recovery Controller (ARC).

Preise für die Routing-Steuerung in ARC

Für die Routingsteuerung in ARC zahlen Sie pro Stunde pro Cluster, den Sie erstellen. Jeder Cluster kann mehrere Routing-Steuerelemente hosten, mit denen Sie Anwendungsfailover auslösen können.

Um die Kosten im Griff zu behalten und die Effizienz zu verbessern, können Sie die kontenübergreifende Nutzung für einen Cluster einrichten, um einen Cluster mit mehreren AWS Konten gemeinsam zu nutzen. Weitere Informationen finden Sie unter Kontoübergreifende Support für Cluster in ARC.

Detaillierte Preisinformationen für ARC und Preisbeispiele finden Sie unter ARC-Preise.

Erste Schritte mit der Wiederherstellung mehrerer Regionen in Amazon Application Recovery Controller (ARC)

Um ein Failover Ihrer Anwendungen mithilfe der Routing-Steuerung in Amazon Application Recovery Controller (ARC) durchzuführen, benötigen Sie AWS Anwendungen, die sich in mehreren befinden AWS-Regionen. Stellen Sie zunächst sicher, dass Ihre Anwendungen in isolierten Replikaten in jeder Region eingerichtet sind, sodass Sie während eines Ereignisses ein Failover von einer zur anderen durchführen können. Anschließend können Sie Routingkontrollen einrichten, um den Anwendungsdatenverkehr so umzuleiten, dass ein Failover von einer primären Anwendung zu einer sekundären Anwendung erfolgt, sodass die Kontinuität für Ihre Benutzer gewahrt bleibt.

> **Note**
>
> Wenn Sie eine Anwendung haben, die in Availability Zones isoliert ist, sollten Sie die Verwendung von Zonal Shift oder Zonal Autoshift für die Failover-Wiederherstellung in Betracht ziehen. Es ist keine Einrichtung erforderlich, um Zonal Shift oder Zonal Autoshift zu verwenden, um Anwendungen nach Beeinträchtigungen in der Availability Zone zuverlässig wiederherzustellen. Weitere Informationen finden Sie unter Verwenden Sie Zonal Shift und Zonal Autoshift, um Anwendungen in ARC wiederherzustellen.

Damit Sie ARC-Routing-Steuerung verwenden können, um Anwendungen während eines Ereignisses wiederherzustellen, empfehlen wir, dass Sie mindestens zwei Anwendungen einrichten, die Kopien voneinander sind. Jedes Replikat oder jede Zelle steht für ein. AWS-Region Nachdem Sie

Ihre Anwendungsressourcen so eingerichtet haben, dass sie den Regionen entsprechen, stellen Sie sicher, dass Ihre Anwendung für eine erfolgreiche Wiederherstellung eingerichtet ist, indem Sie die folgenden Schritte ausführen.

Tipp: Um die Einrichtung zu vereinfachen, stellen AWS CloudFormation wir HashiCorp Terraform-Vorlagen zur Verfügung, mit denen eine Anwendung mit redundanten Replikaten erstellt wird, die unabhängig voneinander ausfallen. Weitere Informationen und das Herunterladen der Vorlagen finden Sie unter. Eine Beispiel-App einrichten

Um sich auf die Verwendung von Routing Control vorzubereiten, stellen Sie sicher, dass Ihre Anwendung so eingerichtet ist, dass sie robust ist. Gehen Sie dazu wie folgt vor:

1. Erstellen Sie unabhängige Kopien Ihres Anwendungsstapels (Netzwerk- und Rechenebene), bei denen es sich in jeder Region um Kopien voneinander handelt, sodass Sie bei einem Ereignis einen Failover des Datenverkehrs von einer zur anderen durchführen können. Stellen Sie sicher, dass Ihr Anwendungscode keine regionsübergreifenden Abhängigkeiten enthält, die dazu führen könnten, dass sich der Ausfall eines Replikats auf das andere auswirkt. Damit ein Failover zwischen beiden erfolgreich ist AWS-Regionen, sollten sich Ihre Stack-Grenzen innerhalb einer Region befinden.
2. Duplizieren Sie alle erforderlichen Stateful-Daten für Ihre Anwendung auf allen Replikaten. Sie können AWS Datenbankdienste verwenden, um Ihre Daten zu replizieren.

Beginnen Sie mit der Routingsteuerung für Datenverkehrs-Failover

Die Routing-Steuerung in Amazon Application Recovery Controller (ARC) ermöglicht es Ihnen, ein Failover für Ihren Datenverkehr auszulösen, sodass ein Failover zwischen redundanten Anwendungskopien oder Replikaten erfolgt, die separat ausgeführt werden. AWS-Regionen Das Failover wird mit DNS unter Verwendung der Amazon Route 53-Datenebene durchgeführt.

Nachdem Sie Ihre Replikate in jeder Region eingerichtet haben, wie im nächsten Abschnitt beschrieben, können Sie jedes Replikat einer Routing-Steuerung zuordnen. Zunächst ordnen Sie die Routingkontrollen den Top-Level-Domainnamen Ihrer Replikate in jeder Region zu. Anschließend fügen Sie der Routingsteuerung eine Zustandsprüfung für die Routingsteuerung hinzu, sodass der Verkehrsfluss ein- und ausgeschaltet werden kann. Auf diese Weise können Sie das Routing des Datenverkehrs zwischen Replikaten Ihrer Anwendung steuern.

Sie können den Status der Routing-Steuerung im AWS Management Console Failover-Verkehr aktualisieren. Wir empfehlen jedoch, stattdessen ARC-Aktionen zu verwenden, indem Sie die API

verwenden oder AWS CLI, um sie zu ändern. API-Aktionen hängen nicht von der Konsole ab und sind daher robuster.

Um beispielsweise ein Failover zwischen Regionen, von us-west-1 bis us-east-1, durchzuführen, können Sie die `update-routing-control-state` API-Aktion verwenden, um den Status von `us-west-1` to und to festzulegen. `Off` `us-east-1` `On`

Bevor Sie Routingsteuerungskomponenten zum Einrichten des Failovers für Ihre Anwendung erstellen, stellen Sie sicher, dass Ihre Anwendung in regionalen Replikaten isoliert ist, sodass Sie ein Failover von einem zum anderen durchführen können. In den nächsten Abschnitten erfahren Sie mehr darüber und erfahren Sie, wie Sie eine neue Anwendung isolieren oder einen Beispielstapel erstellen können.

Eine Beispiel-App einrichten

Damit Sie besser verstehen, wie die Routing-Steuerung funktioniert, stellen wir eine Beispielanwendung mit dem Namen zur Verfügung`TicTacToe`. In diesem Beispiel werden AWS CloudFormation Vorlagen verwendet, um den Vorgang zu vereinfachen, sowie eine herunterladbare AWS CloudFormation Vorlage, sodass Sie sich schnell selbst mit der Einrichtung und Verwendung von ARC vertraut machen können.

Nachdem Sie die Beispiel-App bereitgestellt haben, können Sie die Vorlagen verwenden, um ARC-Komponenten zu erstellen. Anschließend können Sie die Verwendung von Routing-Steuerelementen zur Verwaltung des Datenverkehrs zur App ausprobieren. Sie können die Vorlage und den Prozess an Ihr eigenes Szenario und Ihre eigenen Anwendungen anpassen.

Informationen zu den ersten Schritten mit einer Beispielanwendung und AWS CloudFormation Vorlagen finden Sie in den README-Anweisungen im GitHubARC-Repo. Weitere Informationen zur Verwendung von AWS CloudFormation Vorlagen finden Sie in den AWS CloudFormation Konzepten im AWS CloudFormation Benutzerhandbuch.

Bewährte Methoden für die Routingsteuerung in ARC

Wir empfehlen die folgenden bewährten Methoden für die Wiederherstellung und Failover-Vorbereitung für die Routingsteuerung in ARC.

Topics

- Bewahren Sie speziell entwickelte, AWS langlebige Anmeldeinformationen sicher und stets zugänglich auf

- Wählen Sie niedrigere TTL-Werte für DNS-Einträge, die am Failover beteiligt sind
- Begrenzen Sie die Zeit, in der Clients mit Ihren Endpunkten verbunden bleiben
- Setzen Sie ein Lesezeichen oder codieren Sie Ihre fünf regionalen Cluster-Endpunkte und die Routing-Steuerung fest ARNs
- Wählen Sie nach dem Zufallsprinzip einen Ihrer Endpunkte aus, um den Status Ihrer Routing-Steuerung zu aktualisieren
- Verwenden Sie die extrem zuverlässige Datenebene-API, um die Status der Routing-Steuerung aufzulisten und zu aktualisieren, nicht die Konsole

Bewahren Sie speziell entwickelte, langlebige AWS Anmeldeinformationen sicher und jederzeit zugänglich auf

Halten Sie in einem Notfallwiederherstellungsszenario (DR) die Systemabhängigkeiten auf ein Minimum, indem Sie einen einfachen Ansatz für den Zugriff auf AWS und die Ausführung von Wiederherstellungsaufgaben verwenden. Erstellen Sie langlebige IAM-Anmeldeinformationen speziell für DR-Aufgaben und bewahren Sie die Anmeldeinformationen sicher in einem lokalen physischen Safe oder einem virtuellen Tresor auf, damit Sie bei Bedarf darauf zugreifen können. Mit IAM können Sie Sicherheitsanmeldedaten wie Zugriffsschlüssel und Berechtigungen für den Zugriff auf Ressourcen zentral verwalten. AWS Für Aufgaben, bei denen es sich nicht um DR-Aufgaben handelt, empfehlen wir, weiterhin Verbundzugriff zu verwenden und AWS Dienste wie AWS Single Sign-On zu nutzen.

Um Failover-Aufgaben in ARC mit der Datenebene-API des Wiederherstellungsclusters auszuführen, können Sie Ihrem Benutzer eine ARC-IAM-Richtlinie hinzufügen. Weitere Informationen hierzu finden Sie unter Beispiele für identitätsbasierte Richtlinien in Amazon Application Recovery Controller (ARC).

Wählen Sie niedrigere TTL-Werte für DNS-Einträge, die am Failover beteiligt sind

Für DNS-Einträge, die Sie möglicherweise im Rahmen Ihres Failover-Mechanismus ändern müssen, insbesondere für Datensätze, die einer Integritätsprüfung unterzogen wurden, ist die Verwendung niedrigerer TTL-Werte angemessen. Das Festlegen einer TTL von 60 oder 120 Sekunden ist eine übliche Wahl für dieses Szenario.

Die DNS-TTL-Einstellung (Time to Live) teilt DNS-Resolvern mit, wie lange ein Datensatz zwischengespeichert werden muss, bevor ein neuer angefordert wird. Wenn Sie sich für eine TTL entscheiden, gehen Sie einen Kompromiss zwischen Latenz und Zuverlässigkeit sowie der Reaktionsfähigkeit auf Änderungen ein. Bei einer kürzeren TTL für einen Datensatz bemerken

DNS-Resolver Aktualisierungen des Eintrags schneller, da die TTL angibt, dass sie häufiger Abfragen durchführen müssen.

Weitere Informationen finden Sie unter Auswählen von TTL-Werten für DNS-Einträge in Best Practices für Amazon Route 53 DNS.

Beschränken Sie die Zeit, in der Clients mit Ihren Endpunkten verbunden bleiben

Wenn Sie Routing-Steuerelemente verwenden, um von einem AWS-Region zum anderen zu wechseln, ist der Mechanismus, den Amazon Application Recovery Controller (ARC) verwendet, um Ihren Anwendungsdatenverkehr zu verlagern, ein DNS-Update. Dieses Update bewirkt, dass alle neuen Verbindungen vom beeinträchtigten Standort weggeleitet werden.

Clients mit bereits bestehenden offenen Verbindungen können jedoch weiterhin Anfragen an den beeinträchtigten Standort stellen, bis die Clients wieder eine Verbindung herstellen. Um eine schnelle Wiederherstellung zu gewährleisten, empfehlen wir, die Dauer zu begrenzen, für die Clients mit Ihren Endpunkten verbunden bleiben.

Wenn Sie einen Application Load Balancer verwenden, können Sie mit dieser `keepalive` Option konfigurieren, wie lange Verbindungen bestehen bleiben. Weitere Informationen finden Sie unter Dauer der Keepalive-Dauer des HTTP-Clients im Application Load Balancer Balancer-Benutzerhandbuch.

Standardmäßig legen Application Load Balancer den Wert für die Keepalive-Dauer des HTTP-Clients auf 3600 Sekunden oder 1 Stunde fest. Wir empfehlen Ihnen, den Wert zu senken, um Ihrem Ziel für die Wiederherstellungszeit für Ihre Anwendung zu entsprechen, z. B. 300 Sekunden. Wenn Sie die Dauer einer HTTP-Client-Keepalive-Dauer wählen, sollten Sie berücksichtigen, dass dieser Wert einen Kompromiss darstellt zwischen einer häufigeren Wiederherstellung der Verbindung im Allgemeinen, was sich auf die Latenz auswirken kann, und einer schnelleren Verlagerung aller Clients aus einer beeinträchtigten AZ oder Region.

Fügen Sie Ihren fünf regionalen Cluster-Endpunkten und der Routing-Steuerung ein Lesezeichen hinzu oder schreiben Sie sie fest ARNs

Wir empfehlen, dass Sie eine lokale Kopie Ihrer regionalen ARC-Cluster-Endpunkte in Form von Lesezeichen oder als Automatisierungscode speichern, den Sie verwenden, um Ihre Endpunkte erneut zu testen. Während eines Fehlers können Sie möglicherweise nicht auf einige API-Operationen zugreifen, einschließlich ARC-API-Operationen, die nicht auf dem extrem zuverlässigen Datenebenen-Cluster gehostet werden. Mithilfe der DescribeClusterAPI-Operation können Sie die Endpunkte für Ihre ARC-Cluster auflisten.

Wählen Sie nach dem Zufallsprinzip einen Ihrer Endpunkte aus, um den Status Ihrer Routing-Steuerung zu aktualisieren

Routing-Kontrollen bieten fünf regionale Endpunkte, um selbst bei Ausfällen eine hohe Verfügbarkeit zu gewährleisten. Um ihre volle Resilienz zu erreichen, ist es wichtig, über eine Wiederholungslogik zu verfügen, die bei Bedarf alle fünf Endpunkte verwenden kann. Informationen zur Verwendung von Codebeispielen mit dem AWS SDK, einschließlich Beispielen zum Testen von Cluster-Endpunkten, finden Sie unter. Codebeispiele für Application Recovery Controller mit AWS SDKs

Verwenden Sie die extrem zuverlässige Datenebene-API, um die Status der Routing-Steuerung aufzulisten und zu aktualisieren, nicht die Konsole

Mithilfe der ARC-Datenebene-API können Sie Ihre Routing-Steuerelemente und den Status des ListRoutingControlsVorgangs anzeigen und den Status der Routing-Steuerung aktualisieren, um den Datenverkehr umzuleiten, damit der Failover mit dem UpdateRoutingControlStateVorgang abgeschlossen werden kann. Sie können den AWS CLI (wie in diesen Beispielen) oder den Code verwenden, den Sie mit einem der AWS SDKs geschrieben haben. ARC bietet extreme Zuverlässigkeit mit der API in der Datenebene für den Failover-Verkehr. Wir empfehlen, die API zu verwenden, anstatt den Status der Routing-Steuerung in der zu ändern AWS Management Console.

Stellen Sie eine Connect zu einem Ihrer regionalen Cluster-Endpunkte her, damit ARC die Datenebene-API verwenden kann. Wenn der Endpunkt nicht verfügbar ist, versuchen Sie, eine Verbindung zu einem anderen Cluster-Endpunkt herzustellen.

Wenn eine Sicherheitsregel eine Statusaktualisierung der Routingsteuerung blockiert, können Sie sie umgehen, um die Aktualisierung durchzuführen und den Datenverkehr zu überweisen. Weitere Informationen finden Sie unter Sicherheitsregeln außer Kraft setzen, um den Verkehr umzuleiten.

Testen Sie das Failover mit ARC

Testen Sie das Failover regelmäßig mit ARC-Routing-Steuerung, um ein Failover von Ihrem primären Anwendungsstapel zu einem sekundären Anwendungsstapel durchzuführen. Es ist wichtig, sicherzustellen, dass die ARC-Strukturen, die Sie hinzugefügt haben, auf die richtigen Ressourcen in Ihrem Stack abgestimmt sind und dass alles so funktioniert, wie Sie es erwarten. Sie sollten dies testen, nachdem Sie ARC für Ihre Umgebung eingerichtet haben, und die Tests regelmäßig fortsetzen, damit Ihre Failover-Umgebung vorbereitet ist, bevor es zu einer Ausfallsituation kommt, in der Ihr sekundäres System schnell betriebsbereit sein muss, um Ausfallzeiten für Ihre Benutzer zu vermeiden.

API-Operationen zur Routingsteuerung

Dieser Abschnitt enthält Tabellen mit Listen von API-Vorgängen, die Sie für die Einrichtung und Verwendung der Routing-Steuerung in Amazon Application Recovery Controller (ARC) verwenden können, mit Links zu relevanter Dokumentation.

Beispiele für die Verwendung gängiger API-Operationen zur Konfiguration der Routing-Steuerung mit dem AWS Command Line Interface finden Sie unter Beispiele für die Verwendung von API-Operationen zur ARC-Routingsteuerung mit dem AWS CLI.

In der folgenden Tabelle sind die ARC-API-Operationen aufgeführt, die Sie für die Konfiguration der Routing-Steuerung verwenden können, sowie Links zur entsprechenden Dokumentation.

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Erstellen eines -Clusters	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe CreateCluster
Beschreiben Sie einen Cluster	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe DescribeCluster
Einen Cluster löschen	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe DeleteCluster
Listet Cluster für ein Konto auf	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe ListClusters
Erstellen Sie eine Routing-Steuerung	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe CreateRoutingControl
Beschreiben Sie eine Routingsteuerung	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe DescribeRoutingControl
Aktualisieren Sie eine Routing-Steuerung	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe UpdateRoutingControl
Löschen Sie eine Routingsteuerung	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe DeleteRoutingControl

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Routing-Steuerelemente auflisten	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe ListRoutingControls
Erstellen Sie ein Bedienfeld	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe CreateControlPanel
Beschreiben Sie ein Bedienfeld	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe DescribeControlPanel
Aktualisieren Sie ein Bedienfeld	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe UpdateControlPanel
Löschen Sie ein Control Panel	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe DeleteControlPanel
Bedienfelder auflisten	Siehe Routing-Steuerungskomponenten in ARC erstellen	Siehe ListControlPanels
Erstellen Sie eine Sicherheitsregel	Siehe Sicherheitsregeln für die Routingsteuerung erstellen	Siehe CreateSafetyRule
Beschreiben Sie eine Sicherheitsregel	Siehe Sicherheitsregeln für die Routingsteuerung erstellen	Siehe DescribeSafetyRule
Aktualisieren Sie eine Sicherheitsregel	Siehe Sicherheitsregeln für die Routingsteuerung erstellen	Siehe UpdateSafetyRule
Löschen Sie eine Sicherheitsregel	Siehe Sicherheitsregeln für die Routingsteuerung erstellen	Siehe DeleteSafetyRule
Sicherheitsregeln auflisten	Siehe Sicherheitsregeln für die Routingsteuerung erstellen	Siehe ListSafetyRules
Führen Sie die zugehörigen Route 53-Zustandsprüfungen auf	Siehe Erstellen einer Zustandsprüfung für die Routingsteuerung in ARC	Siehe ListAssociatedRoute53HealthChecks

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Führen Sie die AWS RAM Ressourcenrichtlinien für die gemeinsame Nutzung von Clustern auf	Siehe Kontoübergreifende Support für Cluster in ARC	Siehe GetResourcePolicy

In der folgenden Tabelle sind allgemeine ARC-API-Operationen aufgeführt, die Sie für die Verwaltung des Datenverkehrs-Failovers mit der Routing Control Data Plane verwenden können, sowie Links zur entsprechenden Dokumentation.

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Rufen Sie einen Status der Routing-Steuerung ab	Siehe Status der Routingsteuerung abrufen und aktualisieren in AWS Management Console	Siehe GetRoutingControlState
Routing-Steuerelemente auflisten	N/A	Siehe ListRoutingControls
Aktualisieren Sie den Status einer Routingsteuerung	Siehe Status der Routingsteuerung abrufen und aktualisieren in AWS Management Console	Siehe UpdateRoutingControlState
Aktualisieren Sie mehrere Routingsteuerungsstatus	Siehe Status der Routingsteuerung abrufen und aktualisieren in AWS Management Console	Siehe UpdateRoutingControlStates

Verwenden Sie diesen Dienst mit einem AWS SDK

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK für C++	AWS SDK für C++ Codebeispiele
AWS CLI	AWS CLI Code-Beispiele
AWS SDK für Go	AWS SDK für Go Code-Beispiele
AWS SDK für Java	AWS SDK für Java Code-Beispiele
AWS SDK für JavaScript	AWS SDK für JavaScript Code-Beispiele
AWS SDK für Kotlin	AWS SDK für Kotlin Code-Beispiele
AWS SDK for .NET	AWS SDK for .NET Code-Beispiele
AWS SDK für PHP	AWS SDK für PHP Code-Beispiele
AWS -Tools für PowerShell	Tools für PowerShell Codebeispiele
AWS SDK für Python (Boto3)	AWS SDK für Python (Boto3) Code-Beispiele
AWS SDK für Ruby	AWS SDK für Ruby Code-Beispiele
AWS SDK for Rust	AWS SDK for Rust Code-Beispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Code-Beispiele
AWS SDK for Swift	AWS SDK for Swift Code-Beispiele

Weitere Beispiele speziell für diesen Service finden Sie unter Codebeispiele für Application Recovery Controller mit AWS SDKs.

Beispiel für die Verfügbarkeit

Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Feedback geben auswählen.

Beispiele für die Verwendung von API-Operationen zur ARC-Routingsteuerung mit dem AWS CLI

In diesem Abschnitt werden einfache Anwendungsbeispiele für die Arbeit mit der Routing-Steuerung vorgestellt, wobei die Funktion AWS Command Line Interface zur Verwendung der Routing-Steuerung in Amazon Application Recovery Controller (ARC) mithilfe von API-Operationen verwendet wird. Die Beispiele sollen Ihnen helfen, ein grundlegendes Verständnis für die Arbeit mit der Routingsteuerung mithilfe der CLI zu entwickeln.

Mit der Routing-Steuerung in Amazon Application Recovery Controller (ARC) können Sie Datenverkehrs-Failover zwischen redundanten Anwendungskopien oder Replikaten auslösen, die in separaten AWS-Regionen oder Availability Zones ausgeführt werden.

Sie organisieren Routing-Steuerelemente in Gruppen, die als Control Panels bezeichnet werden und auf einem Cluster bereitgestellt werden. Ein ARC-Cluster ist ein regionaler Satz von Endpunkten, der global bereitgestellt wird. Cluster-Endpunkte bieten eine hochverfügbare API, mit der Sie Routing-Kontrollstatus festlegen und abrufen können. Weitere Informationen zu den Komponenten der Routingsteuerungsfunktion finden Sie unterKomponenten zur Routing-Steuerung .

> **Note**
>
> ARC ist ein globaler Dienst, der mehrere AWS-Regionen Endpunkte unterstützt. In den meisten ARC-CLI-Befehlen müssen Sie jedoch die Region USA West (Oregon) angeben, `--region us-west-2` d. h. den Parameter angeben. Verwenden Sie den `region` Parameter beispielsweise, wenn Sie Wiederherstellungsgruppen, Bedienfelder und Cluster erstellen. Wenn Sie einen Cluster erstellen, stellt ARC Ihnen eine Reihe von regionalen Endpunkten zur Verfügung. Um den Status der Routingsteuerung abzurufen oder zu aktualisieren, müssen Sie den regionalen Endpunkt (die AWS-Region und die Endpunkt-URL) in Ihrem CLI-Befehl angeben.

Weitere Informationen zur Verwendung von finden Sie in der AWS CLI Befehlsreferenz. AWS CLI Eine Liste der API-Aktionen zur Routingsteuerung finden Sie unter API-Operationen zur Routingsteuerung und API-Operationen zur Routingsteuerung.

Wir beginnen mit der Erstellung der Komponenten, die Sie für die Verwaltung des Failovers mithilfe von Routingkontrollen benötigen, und beginnen mit der Erstellung eines Clusters.

Richten Sie Komponenten zur Routing-Steuerung ein

Unser erster Schritt besteht darin, einen Cluster zu erstellen. Ein ARC-Cluster besteht aus fünf Endpunkten, jeweils einer von fünf verschiedenen AWS-Regionen. Die ARC-Infrastruktur unterstützt die Koordination dieser Endpunkte, sodass sie eine hohe Verfügbarkeit und sequentielle Konsistenz der Failover-Operationen gewährleisten.

1. Erstellen eines -Clusters

1a. Erstellen Sie einen Cluster. Das `network-type` ist optional und kann entweder `IPV4` oder sein`DUALSTACK`. Der Standardwert ist `IPV4`.

```
aws route53-recovery-control-config create-cluster --cluster-name test --network-type
 DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

Wenn Sie eine ARC-Ressource zum ersten Mal erstellen, hat sie den Status `PENDING` Während der Clustererstellung. Sie können den Fortschritt überprüfen, indem Sie anrufen`describe-cluster`.

1b. Beschreiben Sie einen Cluster.

```
aws route53-recovery-control-config --region us-west-2 \
    describe-cluster --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

Wenn der Status DEPLOYED lautet, hat ARC den Cluster mit den Endpunkten, mit denen Sie interagieren können, erfolgreich erstellt. Sie können alle Ihre Cluster auflisten, indem Sie anrufen`list-clusters`.

1c. Listen Sie Ihre Cluster auf.

```
aws route53-recovery-control-config --region us-west-2 list-clusters
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

1d. Aktualisieren Sie den Netzwerktyp für Ihre Cluster. Die Optionen sind `IPV4` oder`DUALSTACK`.

```
aws route53-recovery-control-config update-cluster \
--cluster-arn arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234 \
--network-type DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
   "NetworkType": "DUALSTACK"
}
```

2. Erstellen Sie ein Bedienfeld

Ein Bedienfeld ist eine logische Gruppierung zur Organisation Ihrer ARC-Routing-Steuerelemente. Wenn Sie einen Cluster erstellen, stellt ARC automatisch ein Control Panel für Sie bereit. `DefaultControlPanel` Sie können dieses Bedienfeld sofort verwenden.

Ein Control Panel kann nur in einem Cluster existieren. Wenn Sie ein Control Panel in einen anderen Cluster verschieben möchten, müssen Sie es löschen und dann im zweiten Cluster erstellen. Sie

können alle Control Panels in Ihrem Konto einsehen, indem Sie anrufen`list-control-panels`. Um nur die Bedienfelder in einem bestimmten Cluster zu sehen, fügen Sie das `--cluster-arn` Feld hinzu.

2a. Kontrollfelder auflisten.

```
aws route53-recovery-control-config --region us-west-2 \
    list-control-panels --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/eba23304-1a51-4674-ae32-b4cf06070bdd
```

```
{
    "ControlPanels": [
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/1234567dddddd1234567dddddd1234567",
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "DefaultControlPanel": true,
            "Name": "DefaultControlPanel",
            "RoutingControlCount": 0,
            "Status": "DEPLOYED"
        }
    ]
}
```

Erstellen Sie optional Ihr eigenes Control Panel, indem Sie anrufen`create-control-panel`.

2b. Erstellen Sie ein Control Panel.

```
aws route53-recovery-control-config --region us-west-2 create-control-panel \
        --control-panel-name NewControlPanel2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": false,
```

```
        "Name": "NewControlPanel2",
        "RoutingControlCount": 0,
        "Status": "PENDING"
    }
}
```

Wenn Sie eine ARC-Ressource zum ersten Mal erstellen, hat sie den `PENDING` Status „Wird gerade erstellt“. Sie können den Fortschritt überprüfen, indem Sie anrufen`describe-control-panel`.

2c. Beschreiben Sie ein Bedienfeld.

```
aws route53-recovery-control-config --region us-west-2 describe-control-panel \
    --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": true,
        "Name": "DefaultControlPanel",
        "RoutingControlCount": 0,
        "Status": "DEPLOYED"
    }
}
```

3. Erstellen Sie eine Routing-Steuerung

Nachdem Sie den Cluster eingerichtet und sich die Bedienfelder angesehen haben, können Sie mit der Erstellung von Routing-Steuerelementen beginnen. Wenn Sie eine Routing-Steuerung erstellen, müssen Sie mindestens den Amazon-Ressourcennamen (ARN) des Clusters angeben, in dem sich die Routing-Steuerung befinden soll. Sie können auch den ARN eines Control Panels für die Routing-Steuerung angeben. Sie müssen auch den Cluster angeben, in dem sich das Control Panel befindet.

Wenn Sie kein Kontrollfeld angeben, wird Ihre Routing-Steuerung dem automatisch erstellten Bedienfeld hinzugefügt`DefaultControlPanel`.

Erstellen Sie eine Routing-Steuerung, indem Sie anrufen`create-routing-control`.

3a. Erstellen Sie eine Routing-Steuerung.

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
    --routing-control-name NewRc1 \
    --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "RoutingControl": {
        "ControlPanelArn": " arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "PENDING"
    }
}
```

Routing-Steuerelemente folgen demselben Erstellungsmuster wie andere ARC-Ressourcen, sodass Sie ihren Fortschritt verfolgen können, indem Sie eine Beschreibungsoperation aufrufen.

3b. Beschreiben Sie die Routing-Steuerung.

```
aws route53-recovery-control-config --region us-west-2 describe-routing-control \
       --routing-control-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "RoutingControl": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "DEPLOYED"
    }
}
```

Sie können die Routing-Steuerelemente in einem Bedienfeld auflisten, indem Sie anrufen`list-routing-controls`. Das Control Panel ARN ist erforderlich.

3c. Routing-Steuerelemente auflisten.

```
aws route53-recovery-control-config --region us-west-2 list-routing-controls \
        --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "RoutingControls": [
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc1",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
            "Status": "DEPLOYED"
        },
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc2",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
            "Status": "DEPLOYED"
        }
    ]
}
```

Im folgenden Beispiel, in dem wir mit Routingsteuerungsstatus arbeiten, gehen wir davon aus, dass Sie über die beiden in diesem Abschnitt aufgeführten Routingsteuerungen (Rc1 und Rc2) verfügen. In diesem Beispiel stellt jede Routingsteuerung eine Availability Zone dar, in der Ihre Anwendung bereitgestellt wird.

4. Erstellen Sie Sicherheitsregeln

Wenn Sie mit mehreren Routingsteuerungen gleichzeitig arbeiten, entscheiden Sie sich möglicherweise dafür, dass bei deren Aktivierung und Deaktivierung einige Sicherheitsvorkehrungen getroffen werden, um unbeabsichtigte Folgen zu vermeiden, wie z. B. das Ausschalten beider Routingsteuerungen und das Stoppen des gesamten Datenverkehrs. Um diese Schutzmaßnahmen zu erstellen, erstellen Sie Sicherheitsregeln für die Routingsteuerung.

Es gibt zwei Arten von Sicherheitsregeln: Assertion-Regeln und Gating-Regeln. Weitere Informationen zu Sicherheitsregeln finden Sie unter. Sicherheitsregeln für die Routingsteuerung erstellen

Der folgende Aufruf bietet ein Beispiel für die Erstellung einer Assertion-Regel, die sicherstellt, dass zu einem bestimmten Zeitpunkt mindestens eine von zwei Routing-Steuerelementen 0n auf gesetzt ist. Um die Regel zu erstellen, führen Sie sie `create-safety-rule` mit dem `assertion-rule` Parameter aus.

Ausführliche Informationen zum API-Betrieb für Assertionsregeln finden Sie AssertionRuleim Routing Control API-Referenzhandbuch für Amazon Application Recovery Controller.

4a. Erstellen Sie eine Assertion-Regel.

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --assertion-rule '{"Name": "TestAssertionRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "AssertedControls":
        ["arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
        "RuleConfig": {"Threshold": 1, "Type": "ATLEAST", "Inverted": false}}'
```

```
{
    "Rule": {
        "ASSERTION": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/333333444444",
            "AssertedControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestAssertionRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 1,
```

```
                "Type": "ATLEAST"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

Der folgende Aufruf enthält ein Beispiel für die Erstellung einer Gating-Regel, die einen allgemeinen „Ein/Aus“ - oder „Gating“ -Schalter für eine Reihe von Ziel-Routing-Steuerelementen in einem Bedienfeld bereitstellt. Auf diese Weise können Sie die Aktualisierung der Ziel-Routing-Steuerelemente verbieten, sodass beispielsweise die Automatisierung keine unautorisierten Aktualisierungen vornehmen kann. In diesem Beispiel ist der Gating-Switch eine Routing-Steuerung, die durch den `GatingControls` Parameter angegeben wird, und die beiden Routing-Steuerelemente, die gesteuert oder „gesperrt“ werden, werden durch den `TargetControls` Parameter spezifiziert.

> **Note**
>
> Bevor Sie die Gating-Regel erstellen, müssen Sie die Gate-Routing-Steuerung, die keine DNS-Failover-Datensätze enthält, und die Ziel-Routing-Steuerelemente, die Sie mit DNS-Failover-Datensätzen konfigurieren, erstellen.

Um die Regel zu erstellen, führen `create-safety-rule` Sie sie mit dem Parameter aus. `gating-rule`

Ausführliche Informationen zum API-Betrieb für Assertionsregeln finden Sie GatingRuleim Routing Control API-Referenzhandbuch für Amazon Application Recovery Controller.

4b. Erstellen Sie eine Gating-Regel.

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --gating-rule '{"Name": "TestGatingRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "GatingControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
def123def123def"]
```

```
        "TargetControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
ghi456ghi456ghi",
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"],
        "RuleConfig": {"Threshold": 0, "Type": "OR", "Inverted": false}}'
```

```
{
    "Rule": {
        "GATING": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/444444444444",
            "GatingControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
            ],
            "TargetControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"
            ],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestGatingRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 0,
                "Type": "OR"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

Wie bei anderen Ressourcen zur Routingsteuerung können Sie Sicherheitsregeln beschreiben, auflisten oder löschen, nachdem sie auf die Datenebene übertragen wurden.

Nachdem Sie eine oder mehrere Sicherheitsregeln eingerichtet haben, können Sie weiterhin mit dem Cluster interagieren, um den Status für die Routingsteuerung festzulegen oder abzurufen. Wenn ein

`set-routing-control-state` Vorgang gegen eine von Ihnen erstellte Regel verstößt, erhalten Sie eine Ausnahme, die der folgenden ähnelt:

```
Cannot modify control state for [0123456bbbbbbb0123456bbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbb01234563333333444444
```

Die erste Kennung ist der Control-Panel-ARN, der mit dem Routing Control ARN verkettet ist. Die zweite Kennung ist der ARN des Bedienfelds, der mit der Sicherheitsregel ARN verkettet ist.

5. Erstellen Sie Gesundheitschecks

Um Routingkontrollen für den Failover des Datenverkehrs zu verwenden, erstellen Sie Zustandsprüfungen in Amazon Route 53 und verknüpfen die Zustandsprüfungen dann mit Ihren DNS-Einträgen. Für ein Failover des Datenverkehrs legt eine ARC-Routing-Steuerung fest, dass die Zustandsprüfung fehlschlägt, sodass Route 53 den Verkehr umleitet. (Die Integritätsprüfung bestätigt nicht den Zustand Ihrer Anwendung; sie wird lediglich als Methode zur Umleitung des Datenverkehrs verwendet.)

Nehmen wir als Beispiel an, Sie haben zwei Zellen (Regionen oder Availability Zones). Sie konfigurieren eine Zelle als primäre Zelle für Ihre Anwendung und die andere als sekundäre Zelle, auf die ein Failover ausgeführt werden soll.

Um Integritätsprüfungen für Failover einzurichten, können Sie beispielsweise wie folgt vorgehen:

1. Verwenden Sie die ARC-CLI, um eine Routing-Steuerung für jede Zelle zu erstellen.
2. Verwenden Sie die Route 53-CLI, um eine ARC-Zustandsprüfung in Route 53 für jede Routingsteuerung zu erstellen.
3. Verwenden Sie die Route 53-CLI, um zwei Failover-DNS-Einträge in Route 53 zu erstellen und jedem eine Integritätsprüfung zuzuordnen.

5a. Erstellen Sie eine Routing-Steuerung für jede Zelle.

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell1 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell2 \
```

```
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

5b. Erstellen Sie eine Zustandsprüfung für jede Routingsteuerung.

> **Note**
>
> Sie erstellen ARC-Zustandsprüfungen mithilfe der Amazon Route 53-CLI.

```
aws route53 create-health-check --caller-reference RoutingControlCell1 \
        --health-check-config \
        Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell1",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

```
aws route53 create-health-check --caller-reference RoutingControlCell2 \
    --health-check-config \
    Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
```

```
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell2",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

5c. Erstellen Sie zwei Failover-DNS-Einträge und ordnen Sie jedem eine Integritätsprüfung zu.

Sie erstellen Failover-DNS-Einträge in Route 53 mithilfe der Route 53-CLI. Um die Datensätze zu erstellen, folgen Sie den Anweisungen in der Amazon Route AWS CLI 53-Befehlsreferenz für den change-resource-record-setsBefehl. Geben Sie in den Datensätzen den DNS-Wert für jede Zelle zusammen mit dem entsprechenden `HealthCheckID` Wert an, den Route 53 für die Zustandsprüfung erstellt hat (siehe 6b).

Für die primäre Zelle:

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "primary",
    "Failover": "PRIMARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell1.yourdomain.com"
        }
    ],
    "HealthCheckId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

Für die sekundäre Zelle:

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "secondary",
    "Failover": "SECONDARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell2.yourdomain.com"
        }
    ],
    "HealthCheckId": "yyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy"
}
```

Um nun ein Failover von Ihrer primären Zelle zu Ihrer sekundären Zelle durchzuführen, können Sie dem CLI-Beispiel in Schritt 4b folgen, um den Status von `RoutingControlCell1` to `OFF` und `RoutingControlCell2` to zu aktualisieren`ON`.

Auflisten und Aktualisieren von Routingsteuerungen und Status mit dem AWS CLI

Nachdem Sie Ihre Amazon Application Recovery Controller (ARC) -Ressourcen wie Cluster, Routing-Steuerelemente und Control Panels erstellt haben, können Sie mit dem Cluster interagieren, um die Routing-Kontrollstatus für Failover aufzulisten und zu aktualisieren.

Für jeden Cluster, den Sie erstellen, stellt ARC Ihnen eine Reihe von Cluster-Endpunkten zur Verfügung, jeweils einen von fünf. AWS-Regionen Sie müssen einen dieser regionalen Endpunkte (den AWS-Region und die Endpunkt-URL) angeben, wenn Sie den Cluster aufrufen, um den Status der Routing-Steuerung abzurufen oder auf oder zu `On` setzen. `Off` Wenn Sie zum Abrufen oder Aktualisieren von Routingsteuerungsstatus zusätzlich zum regionalen Endpunkt auch den regionalen Endpunkt verwenden, müssen Sie, wie in den Beispielen in diesem Abschnitt gezeigt, auch den regionalen Endpunkt angeben. AWS CLI`--region`

Sie können jeden der regionalen Cluster-Endpunkte verwenden. Wir empfehlen, dass Ihre Systeme abwechselnd die regionalen Endpunkte verwenden und bereit sein, es mit jedem der verfügbaren Endpunkte erneut zu versuchen. Codebeispiele, die veranschaulichen, wie Cluster-Endpunkte nacheinander getestet werden, finden Sie unter. Aktionen für die Verwendung von Application Recovery Controller AWS SDKs

Weitere Informationen zur Verwendung von finden Sie in der AWS CLI Befehlsreferenz. AWS CLI Eine Liste der API-Aktionen zur Routingsteuerung und Links zu weiteren Informationen finden Sie unter API-Operationen zur Routingsteuerung.

> **Important**
>
> Sie können zwar einen Status der Routing-Steuerung auf der Amazon Route 53-Konsole aktualisieren, wir empfehlen jedoch, den Status der Routing-Steuerung mithilfe des AWS CLI oder eines AWS SDK zu aktualisieren. ARC bietet mit der ARC-Routing-Steuerungsdatenebene extreme Zuverlässigkeit für die Umleitung von Datenverkehr und Failover zwischen Zellen. Weitere Empfehlungen zur Verwendung von ARC für Failover finden Sie unter. Bewährte Methoden für die Routingsteuerung in ARC

Wenn Sie eine Routingsteuerung erstellen, wird der Status auf `Off` gesetzt. Das bedeutet, dass der Verkehr nicht an die Zielzelle für diese Routingsteuerung weitergeleitet wird. Sie können den Status der Routingsteuerung überprüfen, indem Sie den Befehl `get-routing-control-state` ausführen.

Um die Region und den Endpunkt zu ermitteln, die angegeben werden sollen, führen Sie den `describe-clusters` Befehl zum Anzeigen von aus`ClusterEndpoints`. Jeder `ClusterEndpoint` enthält eine Region und einen entsprechenden Endpunkt, mit denen Sie den Status der Routingsteuerung abrufen oder aktualisieren können. DescribeClusterist ein API-Vorgang zur Konfiguration der Wiederherstellungssteuerung. Wir empfehlen, dass Sie eine lokale Kopie Ihrer regionalen ARC-Cluster-Endpunkte in Form von Lesezeichen oder fest codiertem Automatisierungscode aufbewahren, den Sie verwenden, um Ihre Endpunkte erneut zu testen.

1. Routing-Steuerelemente auflisten

Sie können Ihre Routingsteuerungen und den Status der Routing-Steuerung mithilfe der äußerst zuverlässigen ARC-Datenebenen-Endpunkte anzeigen.

1. Listet die Routing-Steuerelemente für ein bestimmtes Bedienfeld auf. Wenn Sie kein Control Panel angeben, werden alle Routing-Steuerelemente im Cluster `list-routing-controls` zurückgegeben.

```
aws route53-recovery-cluster list-routing-controls --control-panel-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456 \
```

```
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{
    "RoutingControls": [{
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlName": "RCOne",
        "RoutingControlState": "On"
    },
    {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
zzzzxxxxyyyy123456",
        "RoutingControlName": "RCTwo",
        "RoutingControlState": "Off"
    }
]
```

2. Ruft Routing-Steuerelemente ab

2. Rufen Sie einen Status für die Routingsteuerung ab.

```
aws route53-recovery-cluster get-routing-control-state --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
    "RoutingControlName": "RCOne",
    "RoutingControlState": "On"
```

```
}
```

2. Routingkontrollen aktualisieren

Um den Verkehr an den Zielendpunkt weiterzuleiten, der von der Routingsteuerung gesteuert wird, aktualisieren Sie den Status der Routingsteuerung auf0n. Aktualisieren Sie den Status der Routingsteuerung, indem Sie den Befehl ausführen`update-routing-control-state`. (Wenn die Anfrage erfolgreich ist, ist die Antwort leer.)

2a. Aktualisieren Sie einen Status der Routingsteuerung.

```
aws route53-recovery-cluster update-routing-control-state \
        --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --routing-control-state On \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

Sie können mehrere Routingkontrollen gleichzeitig mit einem API-Aufruf aktualisieren:`update-routing-control-states`. (Wenn die Anfrage erfolgreich ist, ist die Antwort leer.)

2b. Aktualisieren Sie mehrere Status der Routingsteuerung gleichzeitig (Batch-Updates).

```
aws route53-recovery-cluster update-routing-control-states \
        --update-routing-control-state-entries \
        '[{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlState": "Off"}, \
        {"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
        "RoutingControlState": "On"}]' \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

Arbeiten mit Routingsteuerungskomponenten in ARC

Themen

- Routing-Steuerungskomponenten in ARC erstellen
- Status der Routing-Steuerung in ARC anzeigen und aktualisieren
- Sicherheitsregeln für die Routingsteuerung erstellen
- Kontoübergreifende Support für Cluster in ARC

Routing-Steuerungskomponenten in ARC erstellen

In diesem Abschnitt wird erklärt, wie Sie einen Cluster, Routing-Kontrollen, Integritätsprüfungen und Kontrollfelder für die Arbeit mit der Routing-Steuerung in Amazon Application Recovery Controller (ARC) erstellen.

Erstellen Sie zunächst einen Cluster, um Ihre Routing-Kontrollen und die Kontrollfelder, mit denen Sie sie gruppieren, zu hosten. Erstellen Sie anschließend Routingkontrollen und Integritätsprüfungen, sodass Sie den Datenverkehr für ein Failover von einer Zelle zur anderen umleiten können, sodass der Datenverkehr beispielsweise zu Ihrem Backup-Replikat geleitet wird.

Beachten Sie, dass Ihnen für jeden Cluster, den Sie erstellen, stundenweise berechnet wird. In der Regel benötigen Sie nur einen Cluster, um die Routing-Steuerelemente und Bedienfelder für die Verwaltung der Wiederherstellungssteuerung für eine Anwendung zu hosten. Darüber hinaus können Sie die gemeinsame Nutzung von Ressourcen einrichten AWS Resource Access Manager, sodass ein Cluster Routingsteuerungen und andere ARC-Ressourcen hosten kann, die mehreren gehören AWS-Konten. Um mehr über die gemeinsame Nutzung von Ressourcen in ARC zu erfahren, Kontoübergreifende Support für Cluster in ARC. Preisinformationen finden Sie unter Amazon Application Recovery Controller (ARC) — Preise und scrollen Sie nach unten zu Amazon Route 53.

Um Routingkontrollen für den Failover des Datenverkehrs zu verwenden, erstellen Sie Zustandsprüfungen für die Routing-Kontrolle, die Sie mit Amazon Route 53-DNS-Einträgen für Ressourcen in Ihrer Anwendung verknüpfen. Nehmen wir als Beispiel an, Sie haben zwei Zellen, eine, die Sie als primäre Zelle für Ihre Anwendung konfiguriert haben, und die andere, die Sie als sekundäre Zelle konfiguriert haben, auf die ein Failover ausgeführt werden soll.

Gehen Sie wie folgt vor, um Integritätsprüfungen für den Failover einzurichten:

1. Erstellen Sie eine Routingsteuerung für jede Zelle.

2. Erstellen Sie eine Zustandsprüfung für jede Routingsteuerung.
3. Erstellen Sie zwei DNS-Einträge, z. B. zwei DNS-Failover-Einträge, und ordnen Sie jedem Eintrag eine Integritätsprüfung zu.

Ein anderes Szenario, in dem Sie eine Routingsteuerung erstellen könnten, ist die Erstellung einer Sicherheitsregel, bei der es sich um eine Gating-Regel handelt. In diesem Fall ordnen Sie der Routingsteuerung keine Integritätsprüfungen und DNS-Einträge zu, da Sie sie als Gating-Routing-Steuerung verwenden werden. Weitere Informationen finden Sie unter Sicherheitsregeln für die Routingsteuerung erstellen .

In diesen Abschnitten werden die Schritte zum Erstellen der Komponenten für die Routingsteuerung auf der ARC-Konsole beschrieben. Informationen zur Verwendung von API-Operationen zur Konfiguration der Wiederherstellungssteuerung mit ARC finden Sie unter API-Operationen zur Routingsteuerung.

Einen Cluster in ARC erstellen

Sie müssen einen Cluster erstellen, um Routing-Steuerelemente und Bedienfelder in ARC zu hosten.

Ein Cluster besteht aus einer Reihe redundanter regionaler Endpunkte, an denen Sie API-Aufrufe ausführen können, um eine oder mehrere Routing-Steuerelemente zu aktualisieren oder deren Status abzurufen. Ein einzelner Cluster kann eine Reihe von Routing-Steuerelementen hosten.

> **Important**
>
> Beachten Sie, dass Ihnen für jeden Cluster, den Sie erstellen, stundenweise berechnet wird. Ein Cluster kann eine Reihe von Routingsteuerungen und Bedienfeldern für die Verwaltung der Wiederherstellungssteuerung hosten, was in der Regel für eine Anwendung ausreicht.

So erstellen Sie einen Cluster

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Clusters (Cluster) aus.
3. Wählen Sie Create und geben Sie dann einen Namen für Ihren Cluster ein.
4. Wählen Sie Cluster erstellen.

Eine Routing-Steuerung in ARC erstellen

Erstellen Sie eine Routingsteuerung für jede Zelle, zu der Sie den Verkehr weiterleiten möchten. Wenn Sie beispielsweise eine Anwendung mit Ressourcen haben, die Sie aus Gründen der Wiederherstellbarkeit isoliert haben, könnten Sie für jede Anwendung eine Zelle und verschachtelte Zellen für jede AWS-Region Availability Zone innerhalb jeder Region haben. In diesem Szenario würden Sie für jede Zelle und jede verschachtelte Zelle eine Routingsteuerung erstellen.

Beachten Sie beim Erstellen von Routingsteuerungen, dass die Namen der Routingsteuerungen in jedem Bedienfeld eindeutig sein müssen.

Nachdem Sie Routingsteuerungen für die Umleitung von Datenverkehr erstellt haben, verknüpfen Sie jedes Steuerelement mit einer Zustandsprüfung, mit der Sie den Datenverkehr auf der Grundlage der DNS-Einträge, die Sie den einzelnen Zellen zugeordnet haben, an Zellen weiterleiten können. Wenn Sie eine Gating-Regel als Sicherheitsregel einrichten und eine Gating-Routing-Steuerung erstellen, fügen Sie der Routingsteuerung keine Integritätsprüfung hinzu.

Um eine Routing-Steuerung zu erstellen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Routing Control.
3. Wählen Sie auf der Seite „Routing-Steuerung“ die Option „Erstellen“ und wählen Sie dann eine Routing-Steuerung aus.
4. Geben Sie einen Namen für Ihre Routing-Steuerung ein, wählen Sie den Cluster aus, zu dem die Steuerung hinzugefügt werden soll, und wählen Sie, ob Sie sie zu einem vorhandenen Control Panel hinzufügen möchten, einschließlich der Verwendung des Standard-Control-Panels. Oder erstellen Sie ein neues Control Panel.
5. Wenn Sie ein neues Control Panel erstellen möchten, wählen Sie einen Cluster aus, auf dem das Control Panel erstellt werden soll, und geben Sie dann einen Namen für das Panel ein.
6. Wählen Sie „Routing-Steuerung erstellen“.
7. Folgen Sie den Schritten, um die Routing-Steuerung zu benennen und zu erstellen.

Erstellen einer Zustandsprüfung für die Routingsteuerung in ARC

Sie ordnen jeder Routingsteuerung, die Sie für die Umleitung von Verkehr verwenden möchten, eine Zustandsprüfung der Routingsteuerung zu. Anschließend konfigurieren Sie jede Zustandsprüfung mit

einem Amazon Route 53-DNS-Eintrag, z. B. einem Failover-DNS-Eintrag. Anschließend können Sie den Datenverkehr in Amazon Application Recovery Controller (ARC) umleiten, indem Sie einfach den Status der zugehörigen Routing-Steuerung aktualisieren, um sie auf `On` oder `Off` zu setzen.

> **Note**
>
> Sie können eine bestehende Zustandsprüfung der Routing-Kontrolle nicht bearbeiten, um sie einer anderen Routing-Kontrolle zuzuordnen.

Um eine Zustandsprüfung für die Routingsteuerung zu erstellen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Routing Control.
3. Wählen Sie auf der Seite Routing-Steuerung eine Routing-Steuerung aus.
4. Wählen Sie auf der Detailseite der Routingsteuerung die Option Integritätsprüfung erstellen aus.
5. Geben Sie einen Namen für die Integritätsprüfung ein und wählen Sie dann Erstellen aus.

Als Nächstes erstellen Sie Route 53-DNS-Einträge und verknüpfen die einzelnen Einträge mit Ihren Zustandsprüfungen für die Routingsteuerung. Nehmen wir beispielsweise an, dass Sie zwei DNS-Failover-Datensätze verwenden möchten, um Ihre Integritätsprüfungen für die Routingsteuerung zuzuordnen. Damit ARC den Datenverkehr mithilfe von Routingsteuerungen korrekt überführen kann, erstellen Sie zunächst die beiden Failover-Datensätze in Route 53: einen primären und einen sekundären. Weitere Informationen zur Konfiguration von DNS-Failover-Einträgen finden Sie unter Konzepte zur Integritätsprüfung.

Wenn Sie den primären Failover-Datensatz erstellen, sollten die Werte etwa den folgenden entsprechen:

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Primary
Failover: Primary
TTL: 0
Resource Records:
Value: cell1.yourdomain.com
```

```
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Die Werte des sekundären Failover-Datensatzes sollten etwa den folgenden entsprechen:

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Secondary
Failover: Secondary
TTL: 0
Resource Records:
Value: cell2.yourdomain.com
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Nehmen wir nun an, Sie möchten den Verkehr umleiten, weil ein Fehler aufgetreten ist. Dazu aktualisieren Sie die zugehörigen Routingsteuerungsstatus, um den Status der primären Routingsteuerung auf `OFF` und den Status der sekundären Routingsteuerung auf zu `ON` ändern. Wenn Sie dies tun, verhindern die zugehörigen Integritätsprüfungen, dass der Datenverkehr an das primäre Replikat weitergeleitet wird, und leiten ihn stattdessen an das sekundäre Replikat weiter. Weitere Informationen zum Failover von Datenverkehr mithilfe von Routingkontrollen finden Sie unter. Status der Routingsteuerung mithilfe der ARC-API abrufen und aktualisieren (empfohlen)

Beispiele für AWS CLI Befehle zum Erstellen von Routingsteuerungen und den zugehörigen Zustandsprüfungen mithilfe von ARC-API-Vorgängen finden Sie unter Beispiele für die Verwendung von API-Operationen zur ARC-Routingsteuerung mit dem AWS CLI.

Ein Control Panel in ARC erstellen

In einem Control Panel in Amazon Application Recovery Controller (ARC) können Sie verwandte Routing-Steuerelemente gruppieren. Ein Control Panel kann Routing-Steuerelemente enthalten, die je nach Umfang Ihres Failovers einen Microservice innerhalb einer Anwendung, eine gesamte Anwendung selbst oder eine Gruppe von Anwendungen darstellen. Ein Vorteil der Gruppierung von Routing-Steuerelementen in einem Control Panel besteht darin, dass Sie Sicherheitsregeln mit einem Control Panel verwenden können, um Änderungen der Verkehrsführung zu schützen.

Wenn Sie einen Cluster erstellen, erstellt ARC ein Standard-Control-Panel. Sie können das Standard-Bedienfeld für Ihre Routing-Steuerelemente verwenden, oder Sie können ein oder mehrere Bedienfelder erstellen, um Ihre Routing-Steuerelemente zu gruppieren. Beachten Sie, dass für Namen von Bedienfeldern nur ASCII-Zeichen unterstützt werden.

Die Schritte zum Erstellen eines Bedienfelds auf der ARC-Konsole sind in diesem Abschnitt enthalten. Informationen zur Verwendung von API-Operationen zur Konfiguration der Wiederherstellungssteuerung mit ARC finden Sie unter API-Operationen zur Routingsteuerung.

Um ein Control Panel zu erstellen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Routing Control.
3. Wählen Sie auf der Seite „Routing-Steuerung“ die Option „Erstellen“ und anschließend ein Steuerungsfeld aus.
4. Wählen Sie einen Cluster aus, auf dem das Control Panel erstellt werden soll, und geben Sie dann einen Namen für das Panel ein.
5. Wählen Sie „Kontrollpanel erstellen“.

Status der Routing-Steuerung in ARC anzeigen und aktualisieren

In diesem Abschnitt wird beschrieben, wie Sie den Status der Routing-Kontrolle in Amazon Application Recovery Controller (ARC) anzeigen und aktualisieren. Routing-Steuerelemente sind einfache Ein- und Ausschalter, die den Datenfluss zu den Zellen in Ihrer Wiederherstellungsgruppe steuern. Zellen sind in der Regel AWS-Regionen oder manchmal Availability Zones, zu denen auch Ihre Ressourcen gehören. Wenn ein Routingsteuerungsstatus lautet0n, fließt der Verkehr zu der Zelle, die von dieser Routingsteuerung gesteuert wird.

Sie gruppieren Routingsteuerungen in Bedienfeldern, bei denen es sich um logische Failover-Gruppierungen handelt. Wenn Sie beispielsweise ein Control Panel auf der Konsole öffnen, können Sie alle Routing-Steuerelemente für eine Gruppierung gleichzeitig anzeigen, um zu sehen, wohin der Verkehr fließt.

Sie können den Status einer Routing-Steuerung auf der ARC-Konsole oder mithilfe der ARC-API aktualisieren. Wir empfehlen, den Status der Routing-Steuerung mithilfe der API zu aktualisieren. Erstens bietet ARC mit der API in der Datenebene extreme Zuverlässigkeit für die Durchführung dieser Aktionen. Das ist wichtig, wenn Sie diese Status ändern, da bei Änderungen des Routing-Status ein Failover zwischen den einzelnen Zellen erfolgt, indem der Anwendungsdatenverkehr umgeleitet wird. Darüber hinaus können Sie mithilfe der API versuchen, bei Bedarf abwechselnd eine Verbindung zu verschiedenen Cluster-Endpunkten herzustellen, falls ein Cluster-Endpunkt, zu dem Sie eine Verbindung herstellen möchten, nicht verfügbar ist.

Sie können einen Status der Routingsteuerung oder mehrere Status der Routingsteuerung gleichzeitig aktualisieren. Möglicherweise möchten Sie einen Routingsteuerungsstatus auf festlegen, um zu verhindern, dass Datenverkehr `Off` zu einer Zelle fließt, z. B. zu einer Availability Zone, in der bei einer Anwendung eine erhöhte Latenz auftritt. Gleichzeitig möchten Sie möglicherweise einen anderen Status für die Routingsteuerung so einrichten, dass der Verkehr `On` zu einer anderen Zelle oder Availability Zone fließt. In diesem Szenario können Sie beide Routingsteuerungsstatus gleichzeitig aktualisieren, sodass der Verkehr weiterhin fließt.

Themen

- Status der Routingsteuerung mithilfe der ARC-API abrufen und aktualisieren (empfohlen)
- Status der Routingsteuerung abrufen und aktualisieren in AWS Management Console

Status der Routingsteuerung mithilfe der ARC-API abrufen und aktualisieren (empfohlen)

Wir empfehlen Ihnen, API-Operationen von Amazon Application Recovery Controller (ARC) zu verwenden, um den Status der Routing-Steuerung abzurufen oder zu aktualisieren, indem Sie einen AWS CLI Befehl oder Code verwenden, den Sie für die Verwendung von ARC-API-Operationen mit einem der entwickelt haben AWS SDKs. Wir empfehlen, API-Operationen mit der CLI oder im Code zu verwenden, um mit Routingsteuerungszuständen zu arbeiten, anstatt die zu verwenden AWS Management Console.

ARC bietet extreme Zuverlässigkeit beim Failover zwischen Zellen (AWS-Regionen), indem die Routingsteuerungsstatus mithilfe der API aktualisiert werden, da die Routingsteuerungen in einem hochverfügbaren Cluster gespeichert werden. ARC stellt sicher, dass Sie immer auf mindestens drei der fünf regionalen Cluster-Endpunkte zugreifen können, um den Status der Routing-Steuerung zu ändern. Um mithilfe der API einen Status der Routingsteuerung abzurufen oder zu ändern, stellen Sie eine Verbindung zu einem Ihrer regionalen Cluster-Endpunkte her. Wenn der Endpunkt nicht verfügbar ist, können Sie versuchen, eine Verbindung zu einem anderen Ihrer Cluster-Endpunkte herzustellen.

Sie können die Liste der regionalen Cluster-Endpunkte für Ihren Cluster in der Route 53-Konsole oder mithilfe einer API-Aktion anzeigen. DescribeCluster Bei Ihrem Prozess zum Abrufen und Ändern des Status der Routingsteuerung sollten Sie jeden Endpunkt je nach Bedarf abwechselnd überprüfen, da die Cluster-Endpunkte für regelmäßige Wartungs- und Aktualisierungszwecke zwischen den Status „Verfügbar“ und „Nicht verfügbar“ wechseln.

Wir bieten detaillierte Informationen und Codebeispiele für die Verwendung von ARC-API-Operationen zum Abrufen und Aktualisieren von Routingsteuerungsstatus und für die Arbeit mit regionalen Cluster-Endpunkten. Weitere Informationen finden Sie hier:

- Codebeispiele, in denen erklärt wird, wie Sie zwischen regionalen Cluster-Endpunkten rotieren, um den Status der Routing-Steuerung abzurufen und festzulegen, finden Sie unter. Aktionen für die Verwendung von Application Recovery Controller AWS SDKs
- Informationen zur Verwendung von AWS CLI zum Abrufen und Aktualisieren von Routingsteuerungsstatus finden Sie unter Auflisten und Aktualisieren von Routingsteuerungen und Status mit dem AWS CLI.

Status der Routingsteuerung abrufen und aktualisieren in AWS Management Console

Sie können den Status der Routingsteuerung in der abrufen und aktualisieren AWS Management Console. Beachten Sie jedoch, dass Sie in der Konsole keine verschiedenen regionalen Cluster-Endpunkte auswählen können. Das heißt, es gibt keinen Prozess für die Auswahl und Rotation von Cluster-Endpunkten in der Konsole, wie Sie es mit der Amazon Application Recovery Controller (ARC) -API tun können. Darüber hinaus ist die Konsole nicht hochverfügbar, während die ARC-Datenebene extrem zuverlässig ist. Aus diesen Gründen empfehlen wir, die ARC-API zu verwenden, um den Status der Routing-Steuerung für Produktionsabläufe abzurufen und zu aktualisieren.

Weitere Empfehlungen zur Verwendung von ARC für Failover finden Sie unterBewährte Methoden für die Routingsteuerung in ARC.

Gehen Sie wie in den folgenden Verfahren beschrieben vor, um die Routing-Steuerelemente in der Konsole anzuzeigen und zu aktualisieren.

Um den Status der Routingsteuerung abzurufen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Routing Control.
3. Wählen Sie aus der Liste ein Bedienfeld aus und sehen Sie sich die Routing-Steuerelemente an.

Um einen oder mehrere Status der Routing-Steuerung zu aktualisieren

1. Öffnen Sie die Amazon Route 53-Konsole zu https://console.aws.amazon.com/route53/Hause.
2. Wählen Sie unter Application Recovery Controller die Option Routing Control aus.

3. Wählen Sie Aktion und dann Datenverkehrs-Routing ändern aus.
4. Aktualisieren Sie den Status einer oder mehrerer Routing-Steuerelemente auf „`Off`" oder ""`On`, je nachdem, wohin der Datenverkehr für Ihre Anwendung fließen oder beenden soll.“
5. Geben Sie `confirm` in das Textfeld ein.
6. Wählen Sie Verkehrsweiterleitung aktualisieren aus.

Sicherheitsregeln für die Routingsteuerung erstellen

Wenn Sie mit mehreren Routing-Kontrollen gleichzeitig arbeiten, entscheiden Sie sich möglicherweise dafür, Sicherheitsvorkehrungen zu treffen, um unbeabsichtigte Folgen zu vermeiden. Sie möchten beispielsweise verhindern, dass versehentlich alle Routingsteuerungen für eine Anwendung ausgeschaltet werden, was zu einem Fail-Open-Szenario führen würde. Oder Sie möchten vielleicht einen Master-Ein-/Ausschalter implementieren, um eine Reihe von Routingsteuerungen zu deaktivieren, vielleicht um zu verhindern, dass die Automatisierung den Datenverkehr umleitet. Um solche Sicherheitsvorkehrungen für die Routingsteuerung in ARC einzurichten, erstellen Sie Sicherheitsregeln.

Sie konfigurieren Sicherheitsregeln für die Routingsteuerung mit einer Kombination aus Routingkontrollen, Regeln und anderen Optionen, die Sie angeben. Jede Sicherheitsregel ist einem einzelnen Bedienfeld zugeordnet, aber ein Bedienfeld kann mehr als eine Sicherheitsregel haben. Denken Sie beim Erstellen von Sicherheitsregeln daran, dass die Namen der Sicherheitsregeln in jedem Bedienfeld eindeutig sein müssen.

Themen

- Arten von Sicherheitsregeln
- Eine Sicherheitsregel auf der Konsole erstellen
- Eine Sicherheitsregel auf der Konsole bearbeiten oder löschen
- Sicherheitsregeln außer Kraft setzen, um den Verkehr umzuleiten

Arten von Sicherheitsregeln

Es gibt zwei Arten von Sicherheitsregeln: Assertion-Regeln und Gating-Regeln, mit denen Sie Failover auf unterschiedliche Weise schützen können.

Assertion-Regel

Wenn Sie bei einer Assertionsregel einen oder mehrere Status der Routingsteuerung ändern, erzwingt ARC, dass die Kriterien, die Sie bei der Konfiguration der Regel festgelegt haben, erfüllt sind, andernfalls werden die Status der Routing-Steuerung nicht geändert.

Ein Beispiel dafür, wann dies nützlich ist, ist die Verhinderung eines Fail-Open-Szenarios, z. B. eines Szenarios, in dem Sie verhindern, dass der Verkehr zu einer Zelle fließt, aber nicht den Verkehr zu einer anderen Zelle weiterleiten. Um dies zu vermeiden, stellt eine Assertion-Regel sicher, dass mindestens eine Routing-Steuerung in einer Gruppe von Routing-Steuerelementen in einem Control Panel zu einem bestimmten `On` Zeitpunkt aktiviert ist. Dadurch wird sichergestellt, dass der Datenverkehr für eine Anwendung in mindestens eine Region oder Availability Zone fließt.

Einen AWS CLI Beispielbefehl, der eine Assertion-Regel zur Durchsetzung dieser Kriterien erstellt, finden Sie unter Sicherheitsregeln erstellen in Beispiele für die Verwendung von API-Operationen zur ARC-Routingsteuerung mit dem AWS CLI.

Ausführliche Informationen zu den Eigenschaften des API-Vorgangs für Assertionsregeln finden Sie AssertionRuleim Routing Control API-Referenzhandbuch für Amazon Application Recovery Controller.

Gating-Regel

Mit einer Torregel können Sie einen allgemeinen Ein-/Ausschalter für eine Reihe von Routingsteuerungen erzwingen, sodass anhand einer Reihe von Kriterien, die Sie in der Regel angeben, durchgesetzt wird, ob diese Routingsteuerungsstatus geändert werden können. Das einfachste Kriterium ist, ob ein einzelnes Routing-Steuerelement, das Sie als Switch angeben, auf `ON` oder `OFF` eingestellt ist.

Um dies zu implementieren, erstellen Sie eine Gate-Routing-Steuerung, die als Gesamtswitch verwendet wird, und Ziel-Routing-Steuerelemente, um den Verkehrsfluss in verschiedene Regionen oder Availability Zones zu steuern. Um dann manuelle oder automatische Statusaktualisierungen der Ziel-Routing-Steuerelemente zu verhindern, die Sie für die Gating-Regel konfiguriert haben, setzen Sie den Status der Gate-Routing-Steuerung auf. `Off` Um Aktualisierungen zuzulassen, setzen Sie ihn auf. `On`

Einen AWS CLI Beispielbefehl, mit dem eine Torregel erstellt wird, die diese Art von allgemeinem Switch implementiert, finden Sie unter Sicherheitsregeln erstellen in Beispiele für die Verwendung von API-Operationen zur ARC-Routingsteuerung mit dem AWS CLI.

Ausführliche Informationen zu den Eigenschaften der Gating Rule API-Operationen finden Sie GatingRuleim Routing Control API Reference Guide für Amazon Application Recovery Controller.

Eine Sicherheitsregel auf der Konsole erstellen

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Sicherheitsregel auf der ARC-Konsole erstellen. Die Schritte sind ähnlich, unabhängig davon, ob Sie eine Assertion-Regel oder eine Gating-Regel erstellen. Die Unterschiede werden im Verfahren vermerkt.

Weitere Informationen zur Verwendung von API-Vorgängen für Wiederherstellung und Routingsteuerung mit Amazon Application Recovery Controller (ARC) finden Sie unter API-Operationen zur Routingsteuerung.

Um eine Sicherheitsregel zu erstellen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Routing Control.
3. Wählen Sie auf der Seite zur Routing-Steuerung ein Bedienfeld aus.
4. Wählen Sie auf der Detailseite des Bedienfelds Aktion und dann Sicherheitsregel hinzufügen aus.
5. Wählen Sie einen Regeltyp aus, der hinzugefügt werden soll: Assertion-Regel oder Gating-Regel.
6. Wählen Sie einen Namen und ändern Sie optional die Wartezeit.
7. Geben Sie die Konfigurationsoptionen für die Sicherheitsregel an.

   - Geben Sie für eine Assertion-Regel die bestätigten Routing-Kontrollen an.
   - Geben Sie für eine Gating-Regel die Gating-Routing-Steuerung und die Ziel-Routing-Steuerung an.

   Geben Sie für beide Regeln die Regelkonfiguration an, indem Sie den Typ und den Schwellenwert auswählen und angeben, ob die Regel invertiert ist.

   > **Note**
   >
   > Weitere Informationen zur Angabe einer Assertion-Regel finden Sie in den Informationen zur AssertionRuleBedienung im Routing Control API-Referenzhandbuch für Amazon

Application Recovery Controller. Weitere Informationen zur Angabe einer Gating-Regel finden Sie in den Informationen für den GatingRuleVorgang im Routing Control API-Referenzhandbuch für Amazon Application Recovery Controller.

8. Wählen Sie Erstellen aus.

Eine Sicherheitsregel auf der Konsole bearbeiten oder löschen

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Sicherheitsregel auf der ARC-Konsole bearbeiten oder löschen. Sie können nur begrenzte Änderungen an einer Sicherheitsregel vornehmen, um den Namen zu ändern oder die Wartezeit zu aktualisieren. Um weitere Änderungen vorzunehmen, löschen Sie die Sicherheitsregel und erstellen Sie sie neu.

Weitere Informationen zur Verwendung von API-Vorgängen mit Amazon Application Recovery Controller (ARC) finden Sie unter API-Operationen zur Routingsteuerung.

Um eine Sicherheitsregel zu löschen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Routing Control.
3. Wählen Sie auf der Seite zur Routing-Steuerung ein Bedienfeld aus.
4. Wählen Sie auf der Detailseite des Bedienfelds eine Sicherheitsregel aus und klicken Sie dann auf Löschen oder Bearbeiten.

Sicherheitsregeln außer Kraft setzen, um den Verkehr umzuleiten

Es gibt Szenarien, in denen Sie die Sicherheitsvorkehrungen für die Routingsteuerung umgehen möchten, die mit den von Ihnen konfigurierten Sicherheitsregeln durchgesetzt werden. Möglicherweise möchten Sie für die Notfallwiederherstellung schnell ein Failover durchführen und eine oder mehrere Sicherheitsregeln verhindern möglicherweise unerwartet, dass Sie den Status der Routingsteuerung aktualisieren, um den Verkehr umzuleiten. In einem Szenario wie diesem, bei dem das Glas kaputt geht, können Sie eine oder mehrere Sicherheitsregeln außer Kraft setzen, um den Status der Routingsteuerung zu ändern und ein Failover für Ihre Anwendung durchzuführen.

Sie können Sicherheitsregeln umgehen, wenn Sie einen Status der Routingsteuerung (oder mehrere Status der Routingsteuerung) aktualisieren, indem Sie den `update-routing-control-`

`states` AWS CLI Befehl `update-routing-control-state` oder mit dem `safety-rules-to-override` Parameter verwenden. Geben Sie den Parameter mit dem Amazon-Ressourcennamen (ARN) der Sicherheitsregel an, die Sie überschreiben möchten, oder geben Sie eine durch Kommas getrennte Liste an, ARNs um zwei oder mehr Sicherheitsregeln zu überschreiben.

Wenn eine Sicherheitsregel eine Statusaktualisierung der Routingsteuerung blockiert, enthält die Fehlermeldung den ARN der Regel, die das Update blockiert hat. Sie können sich also den ARN notieren und ihn dann in einem CLI-Befehl für den Routing Control State mit dem Parameter Safety Rule Override angeben.

> **Note**
>
> Da für die Routingkontrollen, die Sie aktualisieren, möglicherweise mehr als eine Sicherheitsregel vorhanden ist, könnten Sie den CLI-Befehl ausführen, um Ihren Status der Routingsteuerung mit einer Sicherheitsregelüberschreibung zu aktualisieren, aber die Fehlermeldung erhalten, dass eine andere Sicherheitsregel das Update blockiert. Fügen Sie der Liste der Regeln ARNs , die im Aktualisierungsbefehl außer Kraft gesetzt werden sollen, weiterhin Sicherheitsregeln (getrennt durch Kommas) hinzu, bis der Aktualisierungsbefehl erfolgreich abgeschlossen wurde.

Weitere Informationen zur Verwendung der `SafetyRulesToOverride` Eigenschaft mit der API und finden Sie SDKs unter UpdateRoutingControlState.

Im Folgenden finden Sie zwei Beispiele für CLI-Befehle zum Überschreiben von Sicherheitsregeln, um den Status der Routing-Steuerung zu aktualisieren.

Eine Sicherheitsregel außer Kraft setzen

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
    --routing-control-state On \
    --safety-rules-to-override arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888 \
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Zwei Sicherheitsregeln außer Kraft setzen

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
    --routing-control-state On \
    --safety-rules-to-override "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888" \
    "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
qqqqqqq7777777"
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Kontoübergreifende Support für Cluster in ARC

Amazon Application Recovery Controller (ARC) lässt sich integrieren AWS Resource Access Manager , um die gemeinsame Nutzung von Ressourcen zu ermöglichen. AWS RAM ist ein Service, der es Ihnen ermöglicht, Ressourcen mit anderen zu teilen AWS-Konten oder über AWS Organizations. Für ARC können Sie die Cluster-Ressource gemeinsam nutzen.

Mit können Sie Ressourcen AWS RAM, die Ihnen gehören, gemeinsam nutzen, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe gibt die Ressourcen an, die gemeinsam genutzt werden sollen, und die Teilnehmer, mit denen sie geteilt werden sollen. Zu den Teilnehmern können gehören:

- AWS-Konten Spezifisch innerhalb oder außerhalb der Organisation des Eigentümers in AWS Organizations
- Eine Organisationseinheit innerhalb ihrer Organisation in AWS Organizations
- Ihre gesamte Organisation ist in AWS Organizations

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Durch AWS Resource Access Manager die gemeinsame Nutzung von Cluster-Ressourcen für mehrere Konten in ARC können Sie in einem Cluster Control Panels und Routing-Steuerelemente hosten, die mehreren verschiedenen Benutzern gehören AWS-Konten. Wenn Sie sich dafür entscheiden, einen Cluster gemeinsam zu nutzen, können andere AWS-Konten , von Ihnen

angegebene Cluster als Host für ihre eigenen Control Panels und Routing-Steuerelemente verwenden, was mehr Kontrolle und Flexibilität bei den Routing-Funktionen zwischen verschiedenen Teams ermöglicht.

AWS RAM ist ein Service, der AWS Kunden dabei unterstützt, Ressourcen auf sichere Weise gemeinsam zu nutzen AWS-Konten. Mit AWS RAM können Sie Ressourcen innerhalb einer Organisation oder von Organisationseinheiten (OUs) gemeinsam nutzen AWS Organizations, indem Sie IAM-Rollen und -Benutzer verwenden. AWS RAM ist eine zentralisierte und kontrollierte Methode zur gemeinsamen Nutzung eines Clusters.

Wenn Sie einen Cluster gemeinsam nutzen, können Sie die Gesamtzahl der Cluster reduzieren, die Ihre Organisation benötigt. Mit einem gemeinsam genutzten Cluster können Sie die Gesamtkosten für den Betrieb des Clusters auf verschiedene Teams verteilen, um die Vorteile von ARC bei geringeren Kosten zu maximieren. (Das Erstellen von Ressourcen, die in einem Cluster gehostet werden, ist weder für den Eigentümer noch für die Teilnehmer mit zusätzlichen Kosten verbunden.) Die gemeinsame Nutzung von Clustern für mehrere Konten kann auch das Onboarding mehrerer Anwendungen in ARC vereinfachen, insbesondere wenn Sie über eine große Anzahl von Anwendungen verfügen, die auf mehrere Konten und Betriebsteams verteilt sind.

Um mit der kontenübergreifenden gemeinsamen Nutzung in ARC zu beginnen, erstellen Sie eine gemeinsame Nutzung von Ressourcen in. AWS RAM Die Ressourcenfreigabe gibt Teilnehmer an, die berechtigt sind, den Cluster, der Ihrem Konto gehört, gemeinsam zu nutzen. Anschließend können die Teilnehmer Ressourcen wie Bedienfelder und Routingsteuerungen im Cluster erstellen, indem sie das AWS Management Console oder verwenden, indem sie ARC-API-Operationen mithilfe von AWS Command Line Interface oder ausführen AWS SDKs.

In diesem Thema wird erklärt, wie Sie Ressourcen, die Ihnen gehören, gemeinsam nutzen und wie Sie Ressourcen verwenden, die mit Ihnen geteilt wurden.

Inhalt

- Voraussetzungen für die gemeinsame Nutzung von Clustern
- Einen Cluster gemeinsam nutzen
- Die gemeinsame Nutzung eines gemeinsam genutzten Clusters aufheben
- Identifizieren eines gemeinsam genutzten Clusters
- Verantwortlichkeiten und Berechtigungen für gemeinsam genutzte Cluster
- Kosten für die Abrechnung
- Kontingente

Voraussetzungen für die gemeinsame Nutzung von Clustern

- Um einen Cluster gemeinsam zu nutzen, müssen Sie ihn in Ihrem besitzen AWS-Konto. Das bedeutet, dass die Ressource Ihrem Konto zugewiesen oder bereitgestellt werden muss. Sie können einen Cluster, der mit Ihnen geteilt wurde, nicht gemeinsam nutzen.
- Um einen Cluster mit Ihrer Organisation oder einer Organisationseinheit gemeinsam zu nutzen AWS Organizations, müssen Sie das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.

Einen Cluster gemeinsam nutzen

Wenn Sie einen Cluster gemeinsam nutzen, dessen Eigentümer Sie sind, können die Teilnehmer, die Sie für die gemeinsame Nutzung des Clusters angeben, ihre eigenen ARC-Ressourcen im Cluster erstellen und hosten.

Um einen Cluster gemeinsam zu nutzen, müssen Sie ihn zu einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM -Ressource, mit der Sie Ihre Ressourcen in mehreren AWS-Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die Ressourcen an, die gemeinsam genutzt werden sollen, und die Teilnehmer, mit denen sie geteilt werden. Um einen Cluster gemeinsam zu nutzen, können Sie eine neue Ressourcenfreigabe erstellen oder die Ressource zu einer vorhandenen Ressourcenfreigabe hinzufügen. Um eine neue Ressourcenfreigabe zu erstellen, können Sie die AWS RAM Konsole verwenden oder AWS RAM API-Operationen mit dem AWS Command Line Interface oder verwenden AWS SDKs.

Wenn Sie Teil einer Organisation in Ihrer Organisation sind AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten Teilnehmer in Ihrer Organisation automatisch Zugriff auf den gemeinsam genutzten Cluster. Andernfalls erhalten die Teilnehmer eine Einladung, dem Resource Share beizutreten, und erhalten nach Annahme der Einladung Zugriff auf den gemeinsamen Cluster.

Sie können einen Cluster, der Ihnen gehört, mithilfe der AWS RAM Konsole oder mithilfe von AWS RAM API-Operationen mit AWS CLI oder gemeinsam nutzen SDKs.

Um einen Cluster, den Sie besitzen, mithilfe der AWS RAM Konsole gemeinsam zu nutzen

Weitere Informationen finden Sie unter Erstellen einer Ressourcenfreigabe im AWS RAM Benutzerhandbuch.

Um einen Cluster, den Sie besitzen, gemeinsam zu nutzen, verwenden Sie den AWS CLI

Verwenden Sie den create-resource-share-Befehl.

Erteilen von Berechtigungen zur gemeinsamen Nutzung von Clustern

Für die gemeinsame Nutzung von Clustern über mehrere Konten sind Berechtigungen für den IAM-Prinzipal erforderlich, über AWS RAM den der Cluster gemeinsam genutzt wird.

Wir empfehlen, die `AmazonRoute53RecoveryControlConfigFullAccess` verwaltete IAM-Richtlinie zu verwenden, um sicherzustellen, dass Ihre IAM-Prinzipale über die erforderlichen Berechtigungen für die gemeinsame Nutzung und Nutzung gemeinsam genutzter Cluster verfügen.

Die gemeinsame Nutzung eines Clusters mithilfe einer benutzerdefinierten IAM-Richtlinie erfordert `route53-recovery-control-config:PutResourcePolicyroute53-recovery-control-config:GetResourcePolicy`, und `route53-recovery-control-config:DeleteResourcePolicy` Berechtigungen für diesen Cluster. `PutResourcePolicy`und `DeleteResourcePolicy` sind IAM-Aktionen, für die nur Berechtigungen erforderlich sind. Der Versuch, einen Cluster AWS RAM ohne diese Berechtigungen gemeinsam zu nutzen, führt zu einem Fehler.

Weitere Informationen zur AWS Resource Access Manager Verwendung von IAM finden Sie unter Wie AWS Resource Access Manager verwendet IAM im AWS RAM Benutzerhandbuch.

Die gemeinsame Nutzung eines gemeinsam genutzten Clusters aufheben

Wenn Sie die gemeinsame Nutzung eines Clusters aufheben, gilt für Teilnehmer und Eigentümer Folgendes:

- Aktuelle Teilnehmerressourcen sind weiterhin im nicht gemeinsam genutzten Cluster vorhanden.
- Die Teilnehmer können weiterhin den Status der Routingsteuerung im nicht gemeinsam genutzten Cluster aktualisieren, um das Routing für den Anwendungsfailover zu verwalten.
- Die Teilnehmer können im nicht gemeinsam genutzten Cluster keine neuen Ressourcen mehr erstellen.
- Wenn die Teilnehmer immer noch über Ressourcen in einem nicht gemeinsam genutzten Cluster verfügen, kann der Besitzer den gemeinsam genutzten Cluster nicht löschen.

Um die gemeinsame Nutzung eines Clusters, dessen Eigentümer Sie sind, rückgängig zu machen, entfernen Sie ihn aus der Ressourcenfreigabe. Sie können dies mithilfe der AWS RAM Konsole oder mithilfe von AWS RAM API-Operationen mit dem AWS CLI oder SDKs tun.

So heben Sie mithilfe der Konsole die gemeinsame Nutzung eines gemeinsam genutzten Clusters auf, dessen Eigentümer Sie sind AWS RAM

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um die gemeinsame Nutzung eines gemeinsam genutzten Clusters, dessen Eigentümer Sie sind, rückgängig zu machen, verwenden Sie die AWS CLI

Verwenden Sie den disassociate-resource-share-Befehl.

Identifizieren eines gemeinsam genutzten Clusters

Eigentümer und Teilnehmer können gemeinsam genutzte Cluster anhand der Informationen unter identifizieren AWS RAM. Sie können auch Informationen über gemeinsam genutzte Ressourcen mithilfe der ARC-Konsole und abrufen AWS CLI.

Im Allgemeinen finden Sie weitere Informationen zu den Ressourcen, die Sie geteilt haben oder die mit Ihnen geteilt wurden, den Informationen im AWS Resource Access Manager Benutzerhandbuch:

- Als Besitzer können Sie alle Ressourcen, die Sie mit anderen teilen, mithilfe von anzeigen AWS RAM. Weitere Informationen finden Sie unter Ihre geteilten Ressourcen anzeigen in AWS RAM.
- Als Teilnehmer können Sie alle Ressourcen einsehen, die mit Ihnen geteilt wurden, indem Sie AWS RAM. Weitere Informationen finden Sie unter Ihre geteilten Ressourcen anzeigen in AWS RAM.

Als Besitzer können Sie feststellen, ob Sie einen Cluster gemeinsam nutzen, indem Sie die Informationen in den AWS Management Console oder mithilfe der API-Operationen AWS Command Line Interface mit ARC anzeigen.

Mithilfe der Konsole können Sie feststellen, ob ein Cluster, den Sie besitzen, gemeinsam genutzt wird

Auf der AWS Management Console Detailseite für einen Cluster finden Sie den Status der Clusterfreigabe.

Um festzustellen, ob ein Cluster, den Sie besitzen, gemeinsam genutzt wird, verwenden Sie den AWS CLI

Verwenden Sie den Befehl get-resource-policy. Wenn es eine Ressourcenrichtlinie für einen Cluster gibt, gibt der Befehl Informationen über die Richtlinie zurück.

Wenn ein Cluster mit Ihnen gemeinsam genutzt wird, müssen Sie als Teilnehmer die gemeinsame Nutzung in der Regel akzeptieren. Darüber hinaus enthält das Feld Besitzer für den Cluster das Konto des Clusterbesitzers.

Verantwortlichkeiten und Berechtigungen für gemeinsam genutzte Cluster

Berechtigungen für Besitzer

Wenn Sie einen Cluster, dessen Eigentümer Sie sind AWS-Konten, mit anderen teilen, können Teilnehmer, die den Cluster verwenden dürfen, Kontrollfelder, Routing-Steuerelemente und andere Ressourcen im Cluster einrichten.

Als Clusterbesitzer sind Sie für das Erstellen, Verwalten und Löschen von Clustern verantwortlich. Von Teilnehmern erstellte Ressourcen wie Routingkontrollen und Sicherheitsregeln können Sie nicht ändern oder löschen. Sie können beispielsweise eine von einem Teilnehmer erstellte Routingsteuerung nicht aktualisieren, um den Status der Routingsteuerung zu ändern.

Sie können jedoch die Details für Routingkontrollen anzeigen, die von Teilnehmern eines Clusters erstellt wurden, dessen Eigentümer Sie sind. Sie können sich beispielsweise den Status der Routingsteuerung anzeigen lassen, indem Sie mit dem AWS Command Line Interface oder einen API-Vorgang für die ARC-Routingsteuerung aufrufen AWS SDKs.

Wenn Sie Ressourcen ändern müssen, die von Teilnehmern erstellt wurden, können diese in IAM eine Rolle mit Zugriffsberechtigungen für die Ressourcen einrichten und Ihr Konto zu der Rolle hinzufügen.

Berechtigungen für Teilnehmer

Im Allgemeinen können die Teilnehmer Kontrollfelder, Routingkontrollen, Sicherheitsregeln und Integritätsprüfungen erstellen und verwenden, die sie in einem Cluster erstellen, der für sie gemeinsam genutzt wird. Sie können Clusterressourcen im gemeinsam genutzten Cluster nur anzeigen, ändern oder löschen, wenn sie Eigentümer der Ressourcen sind. Beispielsweise können Teilnehmer Sicherheitsregeln für von ihnen erstellte Bedienfelder erstellen und löschen.

Für Teilnehmer gelten die folgenden Einschränkungen:

- Teilnehmer können Control Panels, die von anderen Konten erstellt wurden, nicht ansehen, ändern oder löschen, die einen gemeinsamen Cluster verwenden.
- Teilnehmer können Routingsteuerungen, einschließlich der Status der Routingsteuerung, für Ressourcen, die in einem gemeinsam genutzten Cluster von anderen Konten erstellt wurden, nicht anzeigen, erstellen oder ändern.

- Teilnehmer können keine Sicherheitsregeln erstellen, ändern oder einsehen, die von anderen Konten in einem gemeinsam genutzten Cluster erstellt wurden.
- Teilnehmer können in einem gemeinsam genutzten Cluster keine Ressourcen über das Standard-Kontrollpanel hinzufügen, da es dem Clusterbesitzer gehört.

Wie bereits erwähnt, können die Teilnehmer im Standard-Control-Panel für einen gemeinsam genutzten Cluster keine Routing-Steuerelemente erstellen, da der Clusterbesitzer Eigentümer des Standard-Control-Panels ist. Der Clusterbesitzer kann jedoch eine kontoübergreifende IAM-Rolle erstellen, die Zugriff auf das Standard-Control-Panel für den Cluster gewährt. Anschließend kann der Besitzer einem Teilnehmer die Berechtigungen zur Übernahme der Rolle gewähren, sodass der Teilnehmer auf das Standard-Kontrollpanel zugreifen und es so verwenden kann, wie es der Besitzer in den Berechtigungen der Rolle festgelegt hat.

Kosten für die Abrechnung

Dem Besitzer eines Clusters in ARC werden die mit dem Cluster verbundenen Kosten in Rechnung gestellt. Für Clusterbesitzer oder Teilnehmer fallen keine zusätzlichen Kosten für die Erstellung von Ressourcen an, die in einem Cluster gehostet werden.

Ausführliche Preisinformationen und Beispiele finden Sie unter Amazon Application Recovery Controller (ARC) — Preise und scrollen Sie nach unten zu Amazon Application Recovery Controller (ARC).

Kontingente

Alle in einem gemeinsamen Cluster erstellten Ressourcen — einschließlich Ressourcen, die von allen Teilnehmern mit Zugriff auf den gemeinsamen Cluster erstellt wurden — werden auf die für den Cluster geltenden Kontingente und andere Ressourcen, wie z. B. Routing-Kontrollen, angerechnet. Wenn Konten, die die Clusterressource gemeinsam nutzen, ein höheres Kontingent als das Kontingent des Clusterbesitzers haben, haben die Kontingente des Clusterbesitzers Vorrang vor den Kontingenten für die Konten, die gemeinsam genutzt werden.

Um besser zu verstehen, wie das funktioniert, sehen Sie sich die folgenden Beispiele an. Um zu veranschaulichen, wie Kontingente bei der gemeinsamen Nutzung von Ressourcen funktionieren, nehmen wir für diese Beispiele an, dass der Clusterbesitzer Eigentümer ist und ein Konto, mit dem der Cluster geteilt wurde, Teilnehmer ist.

Kontingent in den Bedienfeldern

Kontingente werden für die Gesamtzahl der Control Panels des Besitzers pro Cluster durchgesetzt.

Nehmen wir zum Beispiel an, der Besitzer hat ein Kontingent von 50 für die Anzahl der Control Panels pro Cluster und hat 13 Control Panels im Cluster. Nehmen wir nun an, dass der Teilnehmer die Quote auf 150 gesetzt hat. In diesem Szenario kann der Teilnehmer nur bis zu 37 Control Panels (d. h. 50-13) im gemeinsam genutzten Cluster erstellen.

Wenn andere Konten, die den Cluster gemeinsam nutzen, ebenfalls Control Panels erstellen, werden diese ebenfalls alle auf das Cluster-Gesamtkontingent von 50 Control Panels angerechnet.

Kontingente zur Routing-Kontrolle

Routingkontrollen haben mehrere Kontingente: ein Kontingent pro Control Panel, ein Kontingent pro Cluster und ein Kontingent pro Sicherheitsregel. Die Quoten der Eigentümer haben bei all diesen Kontingenten Vorrang.

Nehmen wir zum Beispiel an, der Besitzer hat ein Kontingent von 300 für die Anzahl der Routingkontrollen pro Cluster und verfügt bereits über 300 Routingkontrollen im Cluster. Nehmen wir nun an, der Teilnehmer hat dieses Kontingent auf 500 festgelegt. In diesem Szenario kann der Teilnehmer keine neuen Routing-Steuerelemente im gemeinsam genutzten Cluster erstellen.

Sicherheitsregeln, Kontingente.

Kontingente werden gemäß den Sicherheitsregeln des Besitzers pro Kontingent im Kontrollpanel durchgesetzt.

Nehmen wir zum Beispiel an, der Eigentümer hat eine Quote von 20 für die Anzahl der Sicherheitsregeln pro Kontrollpanel und der Teilnehmer hat diese Quote auf 80 festgelegt. Da in diesem Szenario die Untergrenze des Besitzers Vorrang hat, kann der Teilnehmer nur bis zu 20 Sicherheitsregeln in einem Control Panel im gemeinsam genutzten Cluster erstellen.

Eine Liste der Kontingente für die Routingsteuerung finden Sie unterKontingente für die Routing-Steuerung.

Protokollierung und Überwachung für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)

Sie können AWS CloudTrail die Routing-Steuerung in Amazon Application Recovery Controller (ARC) zur Überwachung von Mustern verwenden und bei der Behebung von Problemen helfen.

Themen

- Protokollieren von ARC-API-Aufrufen mit AWS CloudTrail

Protokollieren von ARC-API-Aufrufen mit AWS CloudTrail

ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ARC ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für ARC als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der ARC-Konsole und Codeaufrufen für die ARC-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für ARC. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen.

Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an ARC, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

ARC-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in ARC eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für ARC, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt

dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle ARC-Aktionen werden im Recovery Readiness API-Referenzhandbuch für Amazon Application Recovery Controller, im Recovery Control Configuration API-Referenzhandbuch für Amazon Application Recovery Controller und im Routing Control API-Referenzhandbuch für Amazon Application Recovery Controller protokolliert und dokumentiert. CloudTrail Beispielsweise generieren Aufrufe von `UpdateRoutingControlState` und `CreateRecoveryGroup` Aktionen Einträge in den CloudTrail Protokolldateien. `CreateCluster`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

ARC-Ereignisse im Ereignisverlauf anzeigen

CloudTrail ermöglicht es Ihnen, aktuelle Ereignisse im Event-Verlauf einzusehen. Um Ereignisse für ARC-API-Anfragen anzuzeigen, müssen Sie in der Regionsauswahl oben in der Konsole die Option USA West (Oregon) auswählen. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Grundlegendes zu ARC-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateCluster` Aktion zur Konfiguration der Routingsteuerung demonstriert.


```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:iam::111122223333:user/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/smithj",
              "accountId": "111122223333",
              "userName": "smithj"
          },
          "webIdFederationData": {},
          "attributes": {
              "mfaAuthenticated": "false",
              "creationDate": "2021-06-30T04:44:41Z"
          }
      }
  },
  "eventTime": "2021-06-30T04:45:46Z",
  "eventSource": "route53-recovery-control-config.amazonaws.com",
  "eventName": "CreateCluster",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.50",
  "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
  "requestParameters": {
      "ClientToken": "12345abcdef-1234-5678-abcd-12345abcdef",
```

```
      "ClusterName": "XYZCluster"
  },
  "responseElements": {
      "Cluster": {
          "Arn": "arn:aws:route53-recovery-control::012345678901:cluster/abc123456-
aa11-bb22-cc33-abc123456",
          "ClusterArn": "arn:aws:route53-recovery-control::012345678901:cluster/
abc123456-aa11-bb22-cc33-abc123456",
          "Name": "XYZCluster",
          "Status": "PENDING"
      }
  },
  "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
  "eventID": "9cab44ef-0777-41e6-838f-f249example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `UpdateRoutingControlState` Aktion für die Routingsteuerung demonstriert.

```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "AssumedRole",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:sts::111122223333:assumed-role/admin/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/admin",
              "accountId": "111122223333",
              "userName": "admin"
          },
          "webIdFederationData": {},
          "attributes": {
              "mfaAuthenticated": "false",
```

```
                "creationDate": "2021-06-30T04:44:41Z"
            }
        }
    },
    "eventTime": "2021-06-30T04:45:46Z",
    "eventSource": "route53-recovery-control-config.amazonaws.com",
    "eventName": "UpdateRoutingControl",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
    "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
    "requestParameters": {
        "RoutingControlName": "XYZRoutingControl3",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
    },
    "responseElements": {
        "RoutingControl": {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "XYZRoutingControl3",
            "Status": "DEPLOYED",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        }
    },
    "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
    "eventID": "9cab44ef-0777-41e6-838f-f249example",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


Identity and Access Management für die Routingsteuerung

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 ARC-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Inhalt

- So funktioniert die Routing-Steuerung in Amazon Application Recovery Controller (ARC) mit IAM
- Beispiele für identitätsbasierte Richtlinien für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)
- AWS verwaltete Richtlinien für die Routingsteuerung in Amazon Application Recovery Controller (ARC)

So funktioniert die Routing-Steuerung in Amazon Application Recovery Controller (ARC) mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf die Routing-Steuerung in Amazon Application Recovery Controller (ARC) zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Routing-Steuerung verfügbar sind.

IAM-Funktionen, die Sie mit der Routing-Steuerung in Amazon Application Recovery Controller (ARC) verwenden können

IAM-Feature	Unterstützung für die Routing-Steuerung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für ARC

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 ARC-Richtlinien zur Routingsteuerung finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)

Ressourcenbasierte Richtlinien innerhalb der Routingsteuerung

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.

Richtlinienaktionen für die Routingsteuerung

Unterstützt Richtlinienaktionen: Ja

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

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 keinen passenden API-Vorgang 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 ARC-Aktionen für die Routing-Steuerung finden Sie unter Von Amazon Route 53 Recovery Controls definierte Aktionen und durch Amazon Route 53 Recovery Cluster definierte Aktionen in der Service Authorization Reference.

Bei Richtlinienaktionen in ARC zur Routing-Steuerung werden je nach der API, mit der Sie arbeiten, die folgenden Präfixe vor der Aktion verwendet:

```
route53-recovery-control-config
route53-recovery-cluster
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Sie können z. B. Folgendes tun:

```
"Action": [
      "route53-recovery-control-config:action1",
      "route53-recovery-control-config:action2"
         ]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "route53-recovery-control-config:Describe*"
```

Beispiele für identitätsbasierte ARC-Richtlinien für die Routingsteuerung finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)

Richtlinienressourcen für ARC

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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": "*"
```

In der Service Authorization Reference finden Sie die folgenden Informationen zu ARC:

Eine Liste der Ressourcentypen und ihrer Aktionen sowie der Aktionen ARNs, die Sie mit dem ARN jeder Ressource angeben können, finden Sie in den folgenden Themen in der Service Authorization Reference:

- Von Amazon Route 53 Recovery Controls definierte Aktionen
- Von Amazon Route 53 Recovery Cluster definierte Aktionen.

Beispiele für identitätsbasierte ARC-Richtlinien zur Routing-Steuerung finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)

Bedingungsschlüssel für Richtlinien für ARC

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 ARC-Bedingungsschlüssel für die Routingsteuerung finden Sie unter den folgenden Themen in der Service Authorization Reference:

- Zustandstasten für Amazon Route 53 Recovery Controls
- Bedingungsschlüssel für Amazon Route 53 Recovery Cluster

Informationen zu den Aktionen und Ressourcen, die Sie mit einem Bedingungsschlüssel verwenden können, finden Sie in den folgenden Themen in der Service Authorization Reference:

- Eine Liste der Ressourcentypen und ihrer Eigenschaften ARNs finden Sie unter Von Amazon Route 53 Recovery Controls definierte Aktionen und von Amazon Route 53 Recovery Cluster definierte Aktionen.
- Eine Liste der Aktionen, die Sie mit dem ARN jeder Ressource angeben können, finden Sie unter Von Amazon Route 53 Recovery Controls definierte Ressourcen und Von Amazon Route 53 Recovery Cluster definierte Ressourcen.

Beispiele für identitätsbasierte ARC-Richtlinien zur Routing-Steuerung finden Sie unter Beispiele für identitätsbasierte Richtlinien für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)

Zugriffskontrolllisten (ACLs) in ARC

Unterstützt ACLs: Nein

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

Attributbasierte Zugriffskontrolle (ABAC) mit ARC

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt 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 Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

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

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Die ARC-Routingsteuerung umfasst die folgende Unterstützung für ABAC:

- Recovery Control Config unterstützt ABAC.

- Recovery Cluster unterstützt ABAC nicht.

Verwenden temporärer Anmeldeinformationen mit ARC

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 von einer Benutzerrolle zu einer IAM-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.

Serviceübergreifende Prinzipalberechtigungen für ARC

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie eine IAM-Entität (Benutzer oder Rolle) verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Richtlinien erteilen einem Prinzipal-Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen.

Informationen darüber, ob für eine Aktion zusätzliche abhängige Aktionen in einer Richtlinie erforderlich sind, finden Sie unter den folgenden Themen in der Service Authorization Reference:

- Amazon Route 53-Wiederherstellungscluster
- Amazon Route 53-Wiederherstellungskontrollen

Servicerollen für ARC

Unterstützt Servicerollen: Nein

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.

Dienstbezogene Rollen für ARC

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS Dienst verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Mit Diensten verknüpfte Rollen werden in Ihrem AWS Konto angezeigt und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Die Routingsteuerung verwendet keine dienstbezogenen Rollen.

Beispiele für identitätsbasierte Richtlinien für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)

Standardmäßig sind Benutzer und Rollen nicht berechtigt, ARC-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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von ARC definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Application Recovery Controller (ARC) in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Beispiel: Zugriff auf die ARC-Konsole zur Routing-Steuerung
- Beispiele: ARC-API-Aktionen für die Konfiguration der Routing-Steuerung

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand ARC-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 Richtlinienvalidierung mit 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 Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Beispiel: Zugriff auf die ARC-Konsole zur Routing-Steuerung

Um auf die Amazon Application Recovery Controller (ARC) -Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den ARC-Ressourcen in Ihrem aufzulisten und anzuzeigen 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 API 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 ARC-Konsole weiterhin verwenden können, wenn Sie nur den Zugriff auf bestimmte API-Operationen zulassen, fügen Sie den Entitäten außerdem eine `ReadOnly` AWS verwaltete Richtlinie für ARC hinzu. Weitere Informationen finden Sie auf der Seite mit verwalteten ARC-Richtlinien oder unter Hinzufügen von Benutzerberechtigungen im IAM-Benutzerhandbuch.

Um Benutzern vollen Zugriff auf die Funktionen der ARC-Routing-Steuerung über die Konsole zu gewähren, fügen Sie dem Benutzer eine Richtlinie wie die folgende hinzu, damit der Benutzer alle Rechte zur Konfiguration der ARC-Routing-Steuerungsressourcen und -vorgänge erhält:

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-cluster:GetRoutingControlState",
                   "route53-recovery-cluster:UpdateRoutingControlState",
                   "route53-recovery-cluster:UpdateRoutingControlStates",
                   "route53-recovery-control-config:CreateCluster",
                   "route53-recovery-control-config:CreateControlPanel",
                   "route53-recovery-control-config:CreateRoutingControl",
                   "route53-recovery-control-config:CreateSafetyRule",
                   "route53-recovery-control-config:DeleteCluster",
                   "route53-recovery-control-config:DeleteControlPanel",
                   "route53-recovery-control-config:DeleteRoutingControl",
                   "route53-recovery-control-config:DeleteSafetyRule",
                   "route53-recovery-control-config:DescribeCluster",
                   "route53-recovery-control-config:DescribeControlPanel",
                   "route53-recovery-control-config:DescribeSafetyRule",
                   "route53-recovery-control-config:DescribeRoutingControl",
                   "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
                   "route53-recovery-control-config:ListClusters",
                   "route53-recovery-control-config:ListControlPanels",
                   "route53-recovery-control-config:ListRoutingControls",
                   "route53-recovery-control-config:ListSafetyRules",
                   "route53-recovery-control-config:UpdateControlPanel",
                   "route53-recovery-control-config:UpdateRoutingControl",
                   "route53-recovery-control-config:UpdateSafetyRule"
             ],
            "Resource": "*"
        },
                {
            "Effect": "Allow",
            "Action": [
                   "route53:GetHealthCheck",
                   "route53:CreateHealthCheck",
                   "route53:DeleteHealthCheck",
                   "route53:ChangeTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiele: ARC-API-Aktionen für die Konfiguration der Routing-Steuerung

Um sicherzustellen, dass ein Benutzer ARC-API-Aktionen verwenden kann, um mit der ARC-Routing-Steuerungskonfiguration zu arbeiten, fügen Sie eine Richtlinie hinzu, die den API-Vorgängen entspricht, mit denen der Benutzer arbeiten muss, wie unten beschrieben.

Um mit API-Operationen für die Konfiguration der Wiederherstellungssteuerung zu arbeiten, fügen Sie dem Benutzer eine Richtlinie wie die folgende hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-control-config:CreateCluster",
                   "route53-recovery-control-config:CreateControlPanel",
                   "route53-recovery-control-config:CreateRoutingControl",
                   "route53-recovery-control-config:CreateSafetyRule",
                   "route53-recovery-control-config:DeleteCluster",
                   "route53-recovery-control-config:DeleteControlPanel",
                   "route53-recovery-control-config:DeleteRoutingControl",
                   "route53-recovery-control-config:DeleteSafetyRule",
                   "route53-recovery-control-config:DescribeCluster",
                   "route53-recovery-control-config:DescribeControlPanel",
                   "route53-recovery-control-config:DescribeSafetyRule",
                   "route53-recovery-control-config:DescribeRoutingControl",
                   "route53-recovery-control-config:GetResourcePolicy",
                   "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
                   "route53-recovery-control-config:ListClusters",
                   "route53-recovery-control-config:ListControlPanels",
                   "route53-recovery-control-config:ListRoutingControls",
                   "route53-recovery-control-config:ListSafetyRules",
                   "route53-recovery-control-config:ListTagsForResource",
                   "route53-recovery-control-config:UpdateControlPanel",
                   "route53-recovery-control-config:UpdateRoutingControl",
                   "route53-recovery-control-config:UpdateSafetyRule",
                   "route53-recovery-control-config:TagResource",
                   "route53-recovery-control-config:UntagResource"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Um Aufgaben in der ARC-Routing-Steuerung mit der Datenebenen-API für den Wiederherstellungscluster auszuführen, z. B. die Aktualisierung der Routingsteuerungsstatus für einen Failover während eines Notfalls, können Sie Ihrem IAM-Benutzer eine ARC-IAM-Richtlinie wie die folgende hinzufügen.

Der `AllowSafetyRuleOverride` boolesche Wert erteilt die Erlaubnis, Sicherheitsregeln außer Kraft zu setzen, die Sie als Schutzmaßnahmen für Routingkontrollen konfiguriert haben. Diese Berechtigung kann in „Breakglass“ -Szenarien erforderlich sein, um die Sicherheitsvorkehrungen bei Katastrophen oder anderen dringenden Failover-Szenarien zu umgehen. Beispielsweise muss ein Operator für die Notfallwiederherstellung möglicherweise schnell einen Failover durchführen und eine oder mehrere Sicherheitsregeln verhindern möglicherweise unerwartet, dass eine Statusaktualisierung der Routing-Steuerung erforderlich ist, um den Verkehr umzuleiten. Mit dieser Berechtigung kann der Betreiber Sicherheitsregeln angeben, die bei API-Aufrufen zur Aktualisierung des Status der Routingsteuerung außer Kraft gesetzt werden. Weitere Informationen finden Sie unter Sicherheitsregeln außer Kraft setzen, um den Verkehr umzuleiten.

Wenn Sie einem Operator die Verwendung der Datenebene-API für den Wiederherstellungscluster gestatten, aber verhindern möchten, dass Sicherheitsregeln außer Kraft gesetzt werden, können Sie eine Richtlinie wie die folgende mit einem `AllowSafetyRuleOverrides` booleschen Wert an anhängen. `false` Damit der Operator Sicherheitsregeln außer Kraft setzen kann, setzen Sie den `AllowSafetyRuleOverrides` booleschen Wert auf. `true`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-cluster:GetRoutingControlState",
                "route53-recovery-cluster:ListRoutingControls"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlStates",
                "route53-recovery-cluster:UpdateRoutingControlState"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "route53-recovery-cluster:AllowSafetyRulesOverrides": "false"
                }
            }
        }
    ]
}
```

AWS verwaltete Richtlinien für die Routingsteuerung in Amazon Application Recovery Controller (ARC)

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, 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 vom Kunden verwaltete 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.

AWS verwaltete Richtlinie: AmazonRoute 53 RecoveryControlConfigFullAccess

Sie können `AmazonRoute53RecoveryControlConfigFullAccess` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt vollen Zugriff auf Aktionen für die Arbeit mit der Wiederherstellungssteuerungskonfiguration in ARC. Hängen Sie sie IAM-Benutzern und anderen Principals zu, die vollen Zugriff auf die Konfigurationsaktionen für die Wiederherstellungssteuerung benötigen.

Sie können nach eigenem Ermessen Zugriff auf zusätzliche Amazon Route 53-Aktionen hinzufügen, damit Benutzer Zustandsprüfungen für Routingkontrollen erstellen können. Sie könnten beispielsweise die Erlaubnis für eine oder mehrere der folgenden Aktionen gewähren: `route53:GetHealthCheckroute53:CreateHealthCheck`,`route53:DeleteHealthCheck`, und`route53:ChangeTagsForResource`.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonRoute53 RecoveryControlConfigFullAccess in der Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonRoute 53 RecoveryControlConfigReadOnlyAccess

Sie können `AmazonRoute53RecoveryControlConfigReadOnlyAccess` an Ihre IAM-Entitäten anhängen. Es ist nützlich für Benutzer, die Routingsteuerungs- und Sicherheitsregelkonfigurationen einsehen müssen. Diese Richtlinie gewährt nur Lesezugriff auf Aktionen für die Arbeit mit der Wiederherstellungssteuerungskonfiguration in ARC. Diese Benutzer können keine Ressourcen für die Wiederherstellungssteuerung erstellen, aktualisieren oder löschen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonRoute53 RecoveryControlConfigReadOnlyAccess in der Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonRoute 53 RecoveryClusterFullAccess

Sie können `AmazonRoute53RecoveryClusterFullAccess` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt vollen Zugriff auf Aktionen für die Arbeit mit der Cluster-Datenebene in ARC. Ordnen Sie sie IAM-Benutzern und anderen Principals zu, die vollen Zugriff auf die Aktualisierung und das Abrufen von Routing-Kontrollstatus benötigen.

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonRoute53 RecoveryClusterFullAccess in der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AmazonRoute 53 RecoveryClusterReadOnlyAccess

Sie können `AmazonRoute53RecoveryClusterReadOnlyAccess` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt schreibgeschützten Zugriff auf die Cluster-Datenebene in ARC. Diese Benutzer können den Status der Routing-Steuerung abrufen, sie jedoch nicht aktualisieren.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonRoute53 RecoveryClusterReadOnlyAccess in der Referenz für AWS verwaltete Richtlinien.

Updates für AWS verwaltete Richtlinien zur Routingsteuerung

Einzelheiten zu den Aktualisierungen der AWS verwalteten Richtlinien für die Routingsteuerung in ARC seit Beginn der Erfassung dieser Änderungen durch diesen Dienst finden Sie unterAktualisierungen der AWS verwalteten Richtlinien für Amazon Application Recovery Controller (ARC). Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite ARC-Dokumentenverlauf.

Kontingente für die Routing-Steuerung

Die Routing-Steuerung in Amazon Application Recovery Controller (ARC) unterliegt den folgenden Kontingenten (früher als Limits bezeichnet).

Entität	Kontingent
Anzahl Cluster pro Konto	2
Anzahl der Control Panels pro Cluster	50
Anzahl der Routing-Steuerelemente pro Bedienfeld	100
Gesamtzahl der Routing-Steuerelemente (in allen Bedienfeldern) pro Cluster	300
Anzahl der Sicherheitsregeln pro Bedienfeld	20
Anzahl der Routing-Kontrollen pro UpdateRoutingControlStatesBetriebsaufruf	10
Anzahl mutierender API-Aufrufe an einen Cluster-Endpunkt pro Sekunde	3

Bereitschaftsprüfung in ARC

Mit der Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC) können Sie herausfinden, ob Ihre Anwendungen und Ressourcen für die Wiederherstellung vorbereitet sind. Nachdem Sie Ihre AWS Anwendung in ARC modelliert und Bereitschaftsprüfungen erstellt haben, werden bei den Prüfungen kontinuierlich Informationen über Ihre Anwendung überwacht, z. B. AWS Ressourcenkontingente, Kapazität und Netzwerkrouting-Richtlinien. Anschließend können Sie wählen, ob Sie über Änderungen informiert werden möchten, die Ihre Fähigkeit beeinträchtigen würden, ein Failover auf ein Replikat Ihrer Anwendung durchzuführen, um sie nach einem Ereignis wiederherzustellen. Mithilfe von Bereitschaftsprüfungen können Sie kontinuierlich sicherstellen, dass Sie Ihre regionsübergreifenden Anwendungen in einem für den Failover-Verkehr skalierten und konfigurierten Zustand beibehalten können.

In diesem Kapitel wird erklärt, wie Sie Ihre Anwendung in ARC modellieren, um die Struktur einzurichten, die das Funktionieren der Bereitschaftsprüfungen ermöglicht, indem Sie eine Wiederherstellungsgruppe und Zellen erstellen, die Ihre Anwendung beschreiben. Anschließend können Sie die Schritte zum Hinzufügen von Bereitschaftsprüfungen und Bereitschaftsbereichen befolgen, sodass ARC die Bereitschaft Ihrer Anwendung überprüfen kann.

Nachdem Sie Bereitschaftsprüfungen erstellt haben, können Sie den Bereitschaftsstatus Ihrer Ressourcen überwachen. Mithilfe von Bereitschaftsprüfungen können Sie kontinuierlich sicherstellen, dass ein Standby-Anwendungsreplikat und die zugehörigen Ressourcen mit Ihrem Produktionsreplikat übereinstimmen. Dabei werden die Kapazität, die Routing-Richtlinien und andere Konfigurationsdetails Ihrer Produktionsanwendung berücksichtigt. Wenn das Replikat nicht übereinstimmt, können Sie Kapazität hinzufügen oder eine Konfiguration ändern, sodass Ihre Anwendungsreplikate wieder aufeinander abgestimmt sind.

> **Important**
>
> Eignungsprüfungen sind äußerst nützlich, um kontinuierlich zu überprüfen, ob die Konfigurationen der Anwendungsreplikate und der Laufzeitstatus aufeinander abgestimmt sind. Bereitschaftsprüfungen sollten nicht verwendet werden, um festzustellen, ob Ihr Produktionsreplikat fehlerfrei ist, und Sie sollten sich auch nicht auf Bereitschaftsprüfungen als primären Auslöser für ein Failover während eines Katastrophenereignisses verlassen.

Was ist eine Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC)?

Bei einer Bereitschaftsprüfung in ARC wird kontinuierlich (in Intervallen von einer Minute) geprüft, ob die AWS bereitgestellte Kapazität, die Servicekontingenten, die Drosselungsgrenzen sowie die Konfiguration und Versionsunterschiede der in der Prüfung enthaltenen Ressourcen nicht übereinstimmen. Mithilfe von Bereitschaftsprüfungen können Sie über diese Unterschiede informiert werden, sodass Sie sicherstellen können, dass jedes Replikat dieselbe Konfiguration und denselben Laufzeitstatus hat. Bereitschaftsprüfungen stellen zwar sicher, dass Ihre konfigurierten Kapazitäten für alle Replikate konsistent sind, Sie sollten jedoch nicht erwarten, dass sie in Ihrem Namen entscheiden, wie hoch die Kapazität Ihres Replikats sein soll. Sie sollten beispielsweise Ihre Anwendungsanforderungen verstehen, sodass Sie die Größe Ihrer Auto Scaling Scaling-Gruppen so dimensionieren, dass in jedem Replikat genügend Pufferkapazität vorhanden ist, um zu verwalten, falls eine andere Zelle nicht verfügbar ist.

Wenn ARC bei Kontingenten eine Nichtübereinstimmung mit einer Bereitschaftsprüfung feststellt, kann es Maßnahmen ergreifen, um die Kontingente für die Replikate aufeinander abzustimmen, indem es das niedrigere Kontingent so erhöht, dass es dem höheren Kontingent entspricht. Wenn die Kontingente übereinstimmen, wird der Status der Bereitschaftsprüfung angezeigt. `READY` (Beachten Sie, dass dies kein sofortiger Aktualisierungsprozess ist und dass die Gesamtzeit vom jeweiligen Ressourcentyp und anderen Faktoren abhängt.)

Der erste Schritt besteht darin, Bereitschaftsprüfungen einzurichten, um eine Wiederherstellungsgruppe zu erstellen, die Ihre Anwendung repräsentiert. Jede Wiederherstellungsgruppe umfasst Zellen für jede einzelne Einheit oder jedes Replikat Ihrer Anwendung zur Eindämmung von Ausfällen. Als Nächstes erstellen Sie Ressourcensätze für jeden Ressourcentyp in Ihrer Anwendung und ordnen den Ressourcensätzen Bereitschaftsprüfungen zu. Schließlich ordnen Sie die Ressourcen Bereitschaftsbereichen zu, sodass Sie den Bereitschaftsstatus der Ressourcen in einer Wiederherstellungsgruppe (Ihrer Anwendung) oder in einzelnen Zellen (Replikate, bei denen es sich um Regionen oder Availability Zones (AZs)) handelt, abrufen können.

Die Bereitschaft (d. h. `READY` oder`NOT READY`) basiert auf den Ressourcen, die in den Bereich der Bereitschaftsprüfung fallen, und auf den Regeln für einen Ressourcentyp. Für jeden Ressourcentyp gibt es eine Reihe von Bereitschaftsregeln, anhand derer ARC-Prüfungen überprüfen, ob die Ressourcen bereit sind. Ob es sich bei einer Ressource um eine Ressource handelt `READY` oder nicht, hängt davon ab, wie die einzelnen Bereitschaftsregeln definiert sind. Alle Bereitschaftsregeln

bewerten Ressourcen, aber einige vergleichen Ressourcen miteinander und wieder andere beziehen sich auf spezifische Informationen zu jeder Ressource in der Ressourcengruppe.

Durch Hinzufügen von Bereitschaftsprüfungen können Sie den Bereitschaftsstatus auf eine von mehreren Arten überwachen: mit EventBridge, in oder mithilfe von ARC-API-Aktionen. AWS Management Console Sie können auch den Bereitschaftsstatus von Ressourcen in verschiedenen Kontexten überwachen, einschließlich der Bereitschaft von Zellen und der Bereitschaft Ihrer Anwendung. Verwenden Sie die kontoübergreifende Autorisierungsfunktion in ARC, um die Einrichtung und Überwachung verteilter Ressourcen von einem einzigen AWS Konto aus zu vereinfachen.

Überwachung von Anwendungsreplikaten mit Bereitschaftsprüfungen

ARC prüft Ihre Anwendungsreplikate mithilfe von Bereitschaftsprüfungen, um sicherzustellen, dass jedes Replikat dieselbe Konfiguration und denselben Laufzeitstatus hat. Bei einer Eignungsprüfung werden kontinuierlich die AWS Ressourcenkapazität, Konfiguration, AWS Kontingente und Routing-Richtlinien für eine Anwendung geprüft. Anhand dieser Informationen können Sie sicherstellen, dass die Replikate für einen Failover bereit sind. Mithilfe von Bereitschaftsprüfungen können Sie sicherstellen, dass Ihre Wiederherstellungsumgebung so skaliert und konfiguriert ist, dass bei Bedarf ein Failover ausgeführt wird.

In den folgenden Abschnitten finden Sie weitere Informationen zur Funktionsweise der Bereitschaftsprüfung.

Eignungsprüfungen und Ihre Anwendungsreplikate

Um auf die Wiederherstellung vorbereitet zu sein, müssen Sie jederzeit genügend freie Kapazitäten in den Replikaten vorhalten, um den Failover-Verkehr aus einer anderen Availability Zone oder Region aufnehmen zu können. ARC überprüft Ihre Anwendung kontinuierlich (einmal pro Minute), um sicherzustellen, dass Ihre bereitgestellte Kapazität in allen Availability Zones oder Regionen übereinstimmt.

Die Kapazität, die ARC überprüft, umfasst beispielsweise die Anzahl der EC2 Amazon-Instances, Aurora-Lese- und Schreibkapazitätseinheiten und die Größe des Amazon EBS-Volumes. Wenn Sie die Kapazität in Ihrem primären Replikat für Ressourcenwerte erhöhen, aber vergessen, auch die entsprechenden Werte in Ihrem Standby-Replikat zu erhöhen, erkennt ARC die Diskrepanz, sodass Sie die Werte im Standby-Replikat erhöhen können.

> **Important**
>
> Eignungsprüfungen sind am nützlichsten, um kontinuierlich zu überprüfen, ob die Konfigurationen der Anwendungsreplikate und der Laufzeitstatus aufeinander abgestimmt sind. Bereitschaftsprüfungen sollten nicht verwendet werden, um festzustellen, ob Ihr Produktionsreplikat fehlerfrei ist, und Sie sollten sich auch nicht auf Bereitschaftsprüfungen als primären Auslöser für ein Failover während eines Katastrophenereignisses verlassen.

In einer Active-Standby-Konfiguration sollten Sie auf der Grundlage Ihrer Überwachungs- und Integritätsprüfungssysteme Entscheidungen darüber treffen, ob ein Failaway von oder zu einer Zelle durchgeführt werden soll, und Bereitschaftsprüfungen als ergänzenden Service für diese Systeme betrachten. ARC-Bereitschaftsprüfungen sind nicht hochverfügbar, weshalb Sie sich nicht darauf verlassen sollten, dass die Checks bei einem Ausfall zugänglich sind. Darüber hinaus sind die geprüften Ressourcen möglicherweise auch während eines Notfalls nicht verfügbar.

Sie können den Bereitschaftsstatus der Ressourcen Ihrer Anwendung in bestimmten Zellen (AWS Regionen oder Availability Zones) oder für Ihre gesamte Anwendung überwachen. Sie können benachrichtigt werden, wenn sich der Status einer Bereitschaftsprüfung ändert, z. B. in`Not ready`, indem Sie Regeln in erstellen EventBridge. Weitere Informationen finden Sie unter Bereitschaftsprüfung in ARC mit Amazon verwenden EventBridge. Sie können den Bereitschaftsstatus auch in oder mithilfe von API-Vorgängen anzeigen, z. `get-recovery-readiness` B. AWS Management Console Weitere Informationen finden Sie unter API-Operationen zur Bereitschaftsprüfung.

So funktioniert die Bereitschaftsprüfung

ARC prüft Ihre Anwendungsreplikate mithilfe von Bereitschaftsprüfungen, um sicherzustellen, dass jedes Replikat dieselbe Konfiguration und denselben Laufzeitstatus hat.

Um für die Wiederherstellung gewappnet zu sein, müssen Sie beispielsweise jederzeit genügend Reservekapazitäten vorhalten, um den Failover-Verkehr aus einer anderen Availability Zone oder Region aufnehmen zu können. ARC überprüft Ihre Anwendung kontinuierlich (einmal pro Minute), um sicherzustellen, dass Ihre bereitgestellte Kapazität in allen Availability Zones oder Regionen übereinstimmt. Die Kapazität, die ARC überprüft, umfasst beispielsweise die Anzahl der EC2 Amazon-Instances, Aurora-Lese- und Schreibkapazitätseinheiten und die Größe des Amazon EBS-Volumes. Wenn Sie die Kapazität in Ihrem primären Replikat für Ressourcenwerte erhöhen, aber

vergessen, auch die entsprechenden Werte in Ihrem Standby-Replikat zu erhöhen, erkennt ARC die Diskrepanz, sodass Sie die Werte im Standby-Replikat erhöhen können.

> **Important**
>
> Eignungsprüfungen sind am nützlichsten, um kontinuierlich zu überprüfen, ob die Konfigurationen der Anwendungsreplikate und der Laufzeitstatus aufeinander abgestimmt sind. Bereitschaftsprüfungen sollten nicht verwendet werden, um festzustellen, ob Ihr Produktionsreplikat fehlerfrei ist, und Sie sollten sich auch nicht auf Bereitschaftsprüfungen als primären Auslöser für ein Failover während eines Katastrophenereignisses verlassen.

In einer Active-Standby-Konfiguration sollten Sie auf der Grundlage Ihrer Überwachungs- und Integritätsprüfungssysteme Entscheidungen darüber treffen, ob ein Failaway von oder zu einer Zelle durchgeführt werden soll, und Bereitschaftsprüfungen als ergänzenden Service für diese Systeme betrachten. ARC-Bereitschaftsprüfungen sind nicht hochverfügbar, weshalb Sie sich nicht darauf verlassen sollten, dass die Checks bei einem Ausfall zugänglich sind. Darüber hinaus sind die geprüften Ressourcen möglicherweise auch während eines Notfalls nicht verfügbar.

Sie können den Bereitschaftsstatus der Ressourcen Ihrer Anwendung in bestimmten Zellen (AWS Regionen oder Availability Zones) oder für Ihre gesamte Anwendung überwachen. Sie können benachrichtigt werden, wenn sich der Status einer Bereitschaftsprüfung ändert, z. B. in`Not ready`, indem Sie Regeln in erstellen EventBridge. Weitere Informationen finden Sie unter Bereitschaftsprüfung in ARC mit Amazon verwenden EventBridge. Sie können den Bereitschaftsstatus auch in oder mithilfe von API-Vorgängen anzeigen, z. `get-recovery-readiness` B. AWS Management Console Weitere Informationen finden Sie unter API-Operationen zur Bereitschaftsprüfung.

Wie Bereitschaftsregeln den Bereitschaftsstatus bestimmen

ARC-Bereitschaftsprüfungen bestimmen den Bereitschaftsstatus auf der Grundlage der vordefinierten Regeln für jeden Ressourcentyp und der Art und Weise, wie diese Regeln definiert sind. ARC umfasst eine Gruppe von Regeln für jeden Ressourcentyp, den es unterstützt. ARC verfügt beispielsweise über Gruppen von Bereitschaftsregeln für Amazon Aurora Aurora-Cluster, Auto Scaling Scaling-Gruppen usw. Bei einigen Bereitschaftsregeln werden Ressourcen in einem Satz miteinander verglichen, und bei anderen werden spezifische Informationen zu jeder Ressource im Ressourcensatz berücksichtigt.

Sie können Bereitschaftsregeln oder Regelgruppen nicht hinzufügen, bearbeiten oder entfernen. Sie können jedoch einen CloudWatch Amazon-Alarm und eine Bereitschaftsprüfung erstellen, um den Status des Alarms zu überwachen. Sie können beispielsweise einen benutzerdefinierten CloudWatch Alarm erstellen, um die Amazon EKS-Container-Services zu überwachen, und eine Bereitschaftsprüfung erstellen, um den Bereitschaftsstatus des Alarms zu überprüfen.

Sie können alle Bereitschaftsregeln für jeden Ressourcentyp in der AWS Management Console Wenn Sie einen Ressourcensatz erstellen, oder Sie können die Bereitschaftsregeln später einsehen, indem Sie zur Detailseite für einen Ressourcensatz navigieren. Sie können die Bereitschaftsregeln auch im folgenden Abschnitt einsehen:Bereitschaftsregeln in ARC.

Wenn bei einer Bereitschaftsprüfung eine Reihe von Ressourcen anhand einer Reihe von Regeln geprüft wird, bestimmt die Art und Weise, wie die einzelnen Regeln definiert sindREADY, ob das Ergebnis NOT READY für alle Ressourcen gilt oder ob das Ergebnis für verschiedene Ressourcen unterschiedlich ist. Darüber hinaus können Sie den Bereitschaftsstatus auf verschiedene Arten anzeigen. Sie können beispielsweise den Bereitschaftsstatus einer Gruppe von Ressourcen in einer Ressourcengruppe oder eine Zusammenfassung des Bereitschaftsstatus für eine Wiederherstellungsgruppe oder eine Zelle (d. h. eine AWS Region oder Availability Zone, je nachdem, wie Sie Ihre Wiederherstellungsgruppe eingerichtet haben) anzeigen.

Der Wortlaut in jeder Regelbeschreibung erklärt, wie die Ressourcen bewertet werden, um den Bereitschaftsstatus zu ermitteln, wenn diese Regel angewendet wird. Eine Regel ist so definiert, dass jede Ressource oder alle Ressourcen in einer Ressourcengruppe überprüft werden, um festzustellen, ob sie bereit sind. Konkret funktionieren die Regeln wie folgt:

- Die Regel überprüft jede Ressource in der Ressourcengruppe, um sicherzustellen, dass ein Zustand vorliegt.
  - Wenn alle Ressourcen erfolgreich sind, werden alle Ressourcen als READY festgelegt.
  - Wenn eine Ressource ausfällt, wird diese Ressource als gesetztNOT READY, und die anderen Zellen bleiben erhaltenREADY.

  Zum Beispiel: MskClusterState:Prüft jeden Amazon MSK-Cluster, um sicherzustellen, dass er sich in einem ACTIVE bestimmten Zustand befindet.
- Die Regel überprüft alle Ressourcen im Ressourcensatz, um sicherzustellen, dass ein Zustand vorliegt.
  - Wenn der Zustand gewährleistet ist, werden alle Ressourcen als READY festgelegt.
  - Wenn eine der Bedingungen nicht entspricht, werden alle Ressourcen auf gesetztNOT READY.

Zum Beispiel: VpcSubnetCount:Inspiziert alle VPC Subnetze, um sicherzustellen, dass sie dieselbe Anzahl von Subnetzen haben.

- Unkritische Regel: Die Regel überprüft alle Ressourcen in der Ressourcengruppe, um sicherzustellen, dass ein Zustand vorliegt.
  - Schlägt einer fehl, bleibt der Bereitschaftsstatus unverändert. Eine Regel mit diesem Verhalten hat einen Hinweis in der Beschreibung.

  Zum Beispiel: ElbV2CheckAzCount:Prüft jeden Network Load Balancer, um sicherzustellen, dass er nur mit einer Availability Zone verbunden ist. Hinweis: Diese Regel hat keinen Einfluss auf den Bereitschaftsstatus.

Darüber hinaus unternimmt ARC einen zusätzlichen Schritt in Bezug auf Kontingente. Wenn bei einer Bereitschaftsprüfung festgestellt wird, dass die Dienstkontingente (der Höchstwert für die Erstellung und den Betrieb von Ressourcen) für eine unterstützte Ressource nicht in den Zellen übereinstimmen, erhöht ARC automatisch das Kontingent für die Ressource mit dem niedrigeren Kontingent. Dies gilt nur für Kontingente (Grenzwerte). Was die Kapazität angeht, sollten Sie je nach Bedarf zusätzliche Kapazität für Ihre Anwendung hinzufügen.

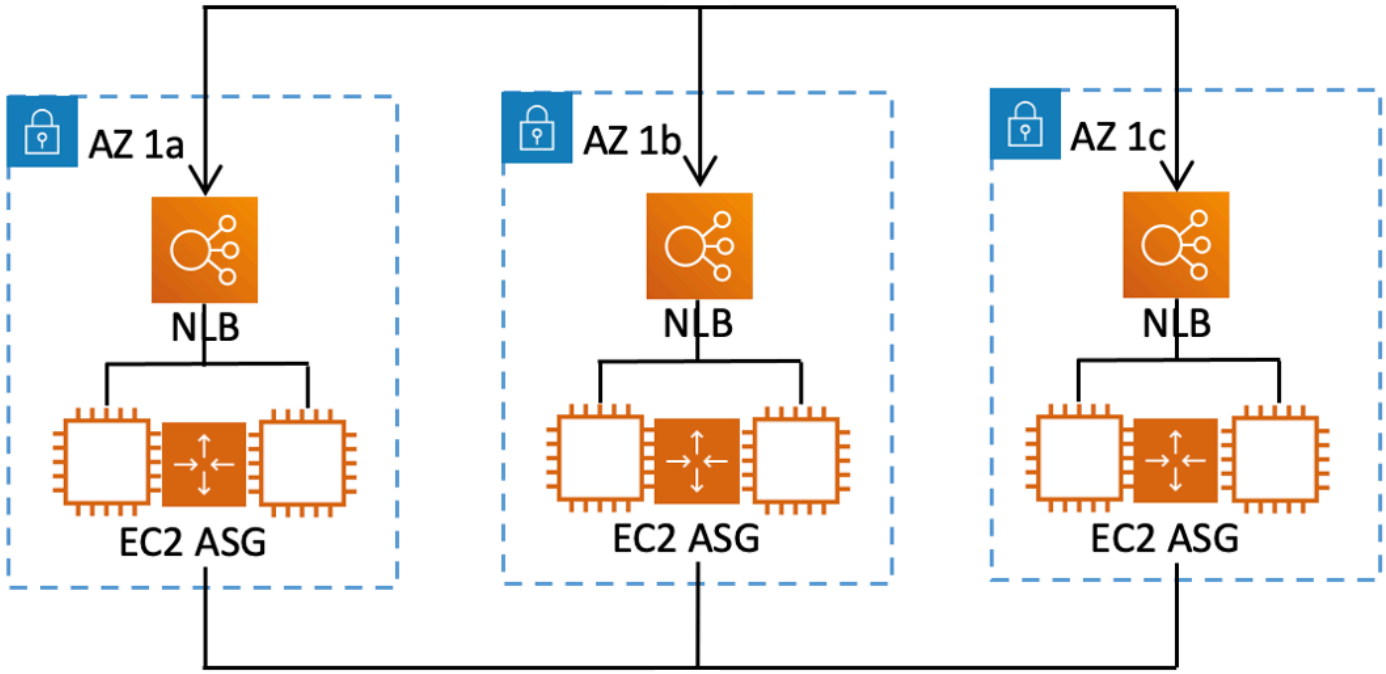
Sie können auch eine EventBridge Amazon-Benachrichtigung für Bereitschaftsprüfungen einrichten, z. B. wenn sich der Status einer Bereitschaftsprüfung auf ändert`NOT READY`. Wenn dann ein Konfigurationskonflikt festgestellt wird, erhalten EventBridge Sie eine Benachrichtigung, sodass Sie Korrekturmaßnahmen ergreifen können, um sicherzustellen, dass Ihre Anwendungsreplikate aufeinander abgestimmt und für die Wiederherstellung vorbereitet sind. Weitere Informationen finden Sie unter Bereitschaftsprüfung in ARC mit Amazon verwenden EventBridge.

Wie Eignungsprüfungen, Ressourcensätze und Bereitschaftsbereiche zusammenarbeiten

Bei Bereitschaftsprüfungen werden immer Gruppen von Ressourcen in Ressourcensätzen geprüft. Sie erstellen Ressourcensätze (separat oder während Sie eine Bereitschaftsprüfung erstellen), um die Ressourcen zu gruppieren, die sich in den Zellen (Availability Zones oder AWS Regions) in Ihrer ARC-Wiederherstellungsgruppe befinden, sodass Sie Bereitschaftsprüfungen definieren können. Ein Ressourcensatz ist in der Regel eine Gruppe desselben Ressourcentyps (wie Network Load Balancer), kann aber auch als DNS-Zielressourcen dienen, um architektonische Eignungsprüfungen durchzuführen.

In der Regel erstellen Sie für jeden Ressourcentyp in Ihrer Anwendung einen Ressourcensatz und prüfen, ob er bereit ist. Für eine Prüfung der architektonischen Eignung erstellen Sie eine DNS-Zielressource der obersten Ebene und einen globalen Ressourcensatz (auf Ebene der Wiederherstellungsgruppe) und anschließend DNS-Zielressourcen auf Zellebene für einen separaten Ressourcensatz.

Das folgende Diagramm zeigt ein Beispiel für eine Wiederherstellungsgruppe mit drei Zellen (Availability Zones), jede mit einem Network Load Balancer (NLB) und einer Auto Scaling Scaling-Gruppe (ASG).



In diesem Szenario würden Sie einen Ressourcensatz und eine Bereitschaftsprüfung für die drei Network Load Balancer und eine Prüfung des Ressourcensatzes und der Bereitschaft für die drei Auto Scaling Scaling-Gruppen erstellen. Jetzt haben Sie eine Eignungsprüfung für jeden Satz von Ressourcen für Ihre Wiederherstellungsgruppe durchgeführt, sortiert nach Ressourcentyp.

Indem Sie Bereitschaftsbereiche für Ressourcen erstellen, können Sie Zusammenfassungen der Bereitschaftsprüfungen für Zellen oder Wiederherstellungsgruppen hinzufügen. Um einen Bereitschaftsbereich für eine Ressource anzugeben, ordnen Sie den ARN der Zelle oder Wiederherstellungsgruppe jeder Ressource in einem Ressourcensatz zu. Sie können dies tun, wenn Sie eine Bereitschaftsprüfung für einen Ressourcensatz erstellen.

Wenn Sie beispielsweise eine Bereitschaftsprüfung für einen Ressourcensatz für die Network Load Balancer für diese Wiederherstellungsgruppe hinzufügen, können Sie jedem NLB gleichzeitig Bereitschaftsbereiche hinzufügen. In diesem Fall würden Sie den ARN von AZ 1a der NLB in AZ 1a, den ARN von der `AZ 1b` NLB `AZ 1b` und den ARN von `AZ 1c` der NLB in zuordnen. `AZ 1c` Wenn Sie eine Bereitschaftsprüfung für die Auto Scaling Scaling-Gruppen erstellen, gehen Sie genauso vor und weisen jeder Gruppe Bereitschaftsbereiche zu, wenn Sie die Eignungsprüfung für den Auto Scaling-Gruppen-Ressourcensatz erstellen.

Es ist optional, Bereitschaftsbereiche zuzuordnen, wenn Sie eine Bereitschaftsprüfung erstellen. Wir empfehlen jedoch dringend, diese Bereiche festzulegen. Mithilfe von Bereitschaftsbereichen kann ARC den korrekten Status `READY` oder den `NOT READY` Bereitschaftsstatus für Bereitschaftsprüfungen mit Zusammenfassung der Wiederherstellungsgruppen und Zusammenfassungen der Bereitschaftsprüfungen auf Zellebene anzeigen. Wenn Sie keine Bereitschaftsbereiche festlegen, kann ARC diese Zusammenfassungen nicht bereitstellen.

Beachten Sie, dass Sie beim Hinzufügen einer Ressource auf Anwendungsebene oder einer globalen Ressource, z. B. einer DNS-Routing-Richtlinie, keine Wiederherstellungsgruppe oder -zelle für den Bereitschaftsbereich auswählen. Stattdessen wählen Sie eine globale Ressource (keine Zelle).

Bereitschaftsprüfungen für DNS-Zielressourcen: Prüfung der Resilienzfähigkeit

Mithilfe von Prüfungen der Verfügbarkeit von DNS-Zielressourcen in ARC können Sie die Architektur- und Resilienzfähigkeit Ihrer Anwendung überprüfen. Diese Art der Bereitschaftsprüfung scannt kontinuierlich die Architektur Ihrer Anwendung und die Routing-Richtlinien von Amazon Route 53, um zonenübergreifende und regionsübergreifende Abhängigkeiten zu prüfen.

Eine wiederherstellungsorientierte Anwendung verfügt über mehrere Replikate, die in Availability Zones oder AWS Regionen isoliert sind, sodass die Replikate unabhängig voneinander ausfallen können. Wenn Ihre Anwendung angepasst werden muss, um korrekt isoliert zu werden, schlägt ARC Änderungen vor, die Sie bei Bedarf vornehmen können, um Ihre Architektur zu aktualisieren und sicherzustellen, dass sie robust und für Failover bereit ist.

ARC erkennt automatisch die Anzahl und den Umfang der Zellen (die Replikate oder Einheiten zur Eindämmung von Ausfällen darstellen) in Ihrer Anwendung und ob die Zellen nach Availability Zone oder Region isoliert sind. Anschließend identifiziert ARC die Anwendungsressourcen in den Zellen und stellt Ihnen Informationen zu diesen zur Verfügung, um festzustellen, ob sie korrekt in Zonen oder Regionen aufgeteilt sind. Wenn Sie beispielsweise Zellen haben, die auf bestimmte Zonen

beschränkt sind, können Sie anhand von Bereitschaftsprüfungen überprüfen, ob Ihre Load Balancer und die dahinter stehenden Ziele ebenfalls in diesen Zonen isoliert sind.

Anhand dieser Informationen können Sie feststellen, ob Sie Änderungen vornehmen müssen, um die Ressourcen in Ihren Zellen den richtigen Zonen oder Regionen zuzuordnen.

Zu Beginn erstellen Sie DNS-Zielressourcen für Ihre Anwendung sowie Ressourcensätze und Bereitschaftsprüfungen für diese Ressourcen. Weitere Informationen finden Sie unter Abrufen von Architekturempfehlungen in ARC.

Bereitschaftsprüfungen und Notfallwiederherstellungsszenarien

ARC-Bereitschaftsprüfungen geben Ihnen Aufschluss darüber, ob Ihre Anwendungen und Ressourcen für die Wiederherstellung bereit sind. Sie helfen Ihnen dabei, sicherzustellen, dass Ihre Anwendungen für den Failover-Verkehr skaliert sind. Der Status der Bereitschaftsprüfung sollte nicht als Signal dafür verwendet werden, dass ein Produktionsreplikat fehlerfrei ist. Sie können jedoch Bereitschaftsprüfungen als Ergänzung zu Ihren Systemen zur Anwendungs- und Infrastrukturüberwachung oder zur Integritätsprüfung verwenden, um festzustellen, ob ein Failaway oder ein Replikat heruntergeladen werden muss.

In einer dringenden Situation oder bei einem Ausfall können Sie anhand einer Kombination aus Integritätsprüfungen und anderen Informationen ermitteln, ob Ihr Standby-Modus hochgefahren und fehlerfrei ist und Sie für den Failover des Produktionsverkehrs bereit sind. Prüfen Sie beispielsweise, ob die Kanarienvögel, die gegen Ihre Standby-Zelle laufen, Ihre Erfolgskriterien erfüllen, und überprüfen Sie zusätzlich, ob der Status der Bereitschaftsüberprüfung für die Standby-Zelle erfüllt ist. `READY`

Beachten Sie, dass ARC-Bereitschaftsprüfungen in einer einzigen AWS Region, USA West (Oregon), durchgeführt werden. Während eines Ausfalls oder einer Katastrophe können die Informationen zur Bereitschaftsüberprüfung veralten oder die Checks nicht mehr verfügbar sein. Weitere Informationen finden Sie unter Daten- und Steuerungsebenen für die Routing-Steuerung.

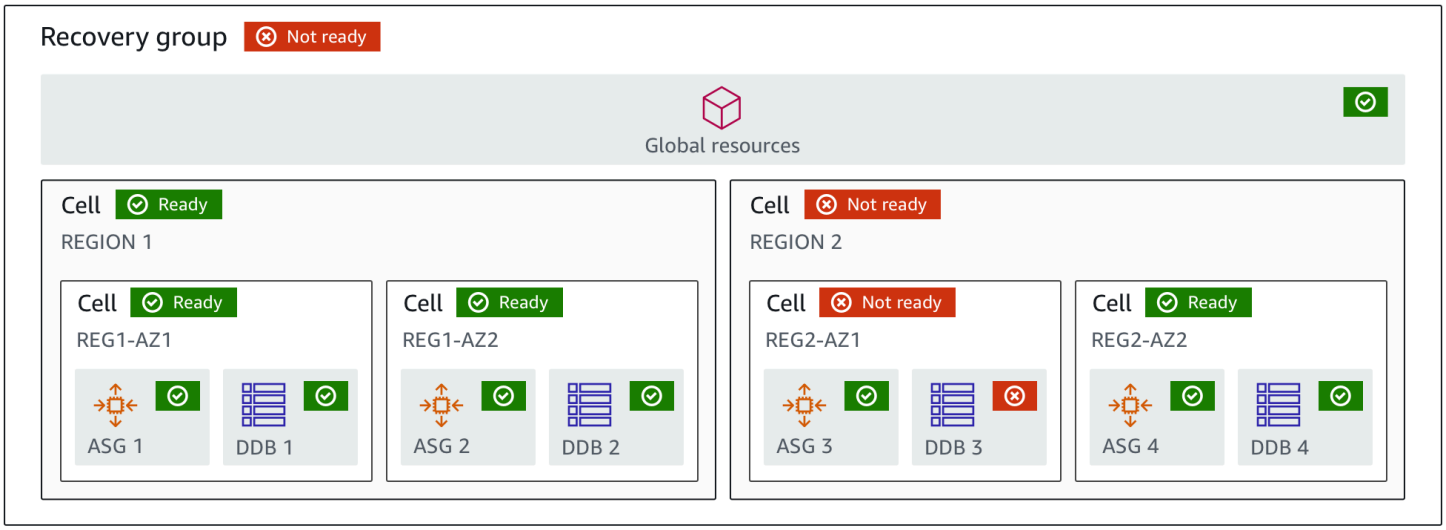
AWS Verfügbarkeit in der Region für Bereitschaftsprüfungen

Detaillierte Informationen zu regionalen Support- und Service-Endpunkten für Amazon Application Recovery Controller (ARC) finden Sie unter Amazon Application Recovery Controller (ARC) - Endpunkte und Kontingente in der Amazon Web Services General Reference.

> **Note**
>
> Die Prüfung der Eignung in Amazon Application Recovery Controller (ARC) ist eine globale Funktion. Ressourcen für die Bereitschaftsprüfung befinden sich jedoch in der Region USA West (Oregon), sodass Sie die Region USA West (Oregon) (den Parameter angeben `--region us-west-2`) in regionalen AWS CLI ARC-Befehlen angeben müssen, z. B. wenn Sie Ressourcen wie Ressourcensätze und Bereitschaftsprüfungen erstellen.

Komponenten der Bereitschaftsprüfung

Das folgende Diagramm zeigt ein Beispiel für eine Wiederherstellungsgruppe, die so konfiguriert ist, dass sie die Funktion zur Prüfung der Bereitschaft unterstützt. In diesem Beispiel sind die Ressourcen in einer Wiederherstellungsgruppe in Zellen (nach AWS-Region) und verschachtelten Zellen (nach Availability Zones) gruppiert. Es gibt einen allgemeinen Bereitschaftsstatus für die Wiederherstellungsgruppe (Anwendung) sowie einen individuellen Bereitschaftsstatus für jede Zelle (Region) und verschachtelte Zelle (Availability Zone).



Im Folgenden sind die Komponenten der Funktion zur Prüfung der Bereitschaft in ARC aufgeführt.

Zelle

Eine Zelle definiert die Replikate oder unabhängigen Failover-Einheiten Ihrer Anwendung. Es gruppiert alle AWS Ressourcen, die für die unabhängige Ausführung Ihrer Anwendung innerhalb des Replikats erforderlich sind. Beispielsweise könnten Sie einen Satz von Ressourcen in einer primären Zelle und einen anderen Satz in einer Standby-Zelle haben. Sie bestimmen die Grenze dessen, was eine Zelle umfasst, aber Zellen stellen in der Regel eine Availability Zone oder eine

Region dar. Sie können mehrere Zellen (verschachtelte Zellen) innerhalb einer Zelle haben, z. B. AZs innerhalb einer Region. Jede verschachtelte Zelle stellt eine isolierte Failover-Einheit dar.

Wiederherstellungsgruppe

Die Zellen werden in einer Wiederherstellungsgruppe zusammengefasst. Eine Wiederherstellungsgruppe steht für eine Anwendung oder Gruppe von Anwendungen, für die Sie die Failover-Bereitschaft überprüfen möchten. Sie besteht aus zwei oder mehr Zellen oder Replikaten, die hinsichtlich ihrer Funktionalität zueinander passen. Wenn Sie beispielsweise über eine Webanwendung verfügen, die über us-east-1a und us-east-1b repliziert wird, wobei us-east-1b Ihre Failover-Umgebung ist, können Sie diese Anwendung in ARC als Wiederherstellungsgruppe mit zwei Zellen darstellen: eine in us-east-1a und eine in us-east-1b. Eine Wiederherstellungsgruppe kann auch eine globale Ressource enthalten, z. B. eine Route 53-Zustandsprüfung.

Ressourcen und Ressourcen-Identifikatoren

Wenn Sie Komponenten für Bereitschaftsprüfungen in ARC erstellen, geben Sie mithilfe einer Ressourcen-ID eine Ressource an, z. B. eine Amazon DynamoDB-Tabelle, einen Network Load Balancer oder eine DNS-Zielressource. Eine Ressourcen-ID ist entweder der Amazon-Ressourcenname (ARN) für die Ressource oder, für eine DNS-Zielressource, die Kennung, die ARC bei der Erstellung der Ressource generiert.

DNS-Zielressource

Eine DNS-Zielressource ist die Kombination aus dem Domainnamen Ihrer Anwendung und anderen DNS-Informationen, z. B. der AWS Ressource, auf die die Domain verweist. Das Hinzufügen einer AWS Ressource ist optional, aber wenn Sie sie angeben, muss es sich um einen Route 53-Ressourceneintrag oder einen Network Load Balancer handeln. Wenn Sie die AWS Ressource bereitstellen, erhalten Sie detailliertere Architekturempfehlungen, mit denen Sie die Ausfallsicherheit Ihrer Anwendung bei der Wiederherstellung verbessern können. Sie können in ARC Ressourcensätze für DNS-Zielressourcen erstellen und anschließend eine Eignungsprüfung für die Ressourcengruppe durchführen, sodass Sie Architekturempfehlungen für Ihre Anwendung erhalten. Bei der Eignungsprüfung wird auch die DNS-Routing-Richtlinie für Ihre Anwendung auf der Grundlage der Bereitschaftsregeln für DNS-Zielressourcen überwacht.

Ressourcensatz

Ein Ressourcensatz ist ein Satz von Ressourcen, einschließlich AWS Ressourcen oder DNS-Zielressourcen, der sich über mehrere Zellen erstreckt. Beispielsweise könnten Sie einen Load Balancer in us-east-1a und einen weiteren in us-east-1b haben. Um die Wiederherstellungsbereitschaft der Load Balancer zu überwachen, können Sie einen

Ressourcensatz erstellen, der beide Load Balancer umfasst, und anschließend eine Bereitschaftsprüfung für den Ressourcensatz durchführen. ARC überprüft kontinuierlich, ob die Ressourcen in der Gruppe bereit sind. Sie können auch einen Bereitschaftsbereich hinzufügen, um Ressourcen in einem Ressourcensatz der Wiederherstellungsgruppe zuzuordnen, die Sie für Ihre Anwendung erstellen.

Bereitschaftsregel

Bereitschaftsregeln sind Prüfungen, die ARC anhand einer Reihe von Ressourcen in einer Ressourcengruppe durchführt. ARC verfügt über eine Reihe von Bereitschaftsregeln für jeden Ressourcentyp, für den es Bereitschaftsprüfungen unterstützt. Jede Regel enthält eine ID und eine Beschreibung, die erklärt, worauf ARC die Ressourcen überprüft.

Prüfung der Bereitschaft

Bei einer Bereitschaftsprüfung wird ein Ressourcensatz in Ihrer Anwendung überwacht, z. B. ein Satz von Amazon Aurora Aurora-Instances, für den ARC die Wiederherstellungsbereitschaft prüft. Zu den Bereitschaftsprüfungen können Prüfungen gehören, beispielsweise Kapazitätskonfigurationen, AWS Kontingente oder Routing-Richtlinien. Wenn Sie beispielsweise die Bereitschaft Ihrer Amazon EC2 Auto Scaling Scaling-Gruppen in zwei Availability Zones überprüfen möchten, können Sie eine Bereitschaftsprüfung für einen Ressourcensatz mit zwei Ressourcen erstellenARNs, eine für jede Auto Scaling Scaling-Gruppe. Um dann sicherzustellen, dass jede Gruppe gleichmäßig skaliert wird, überwacht ARC kontinuierlich die Instance-Typen und die Anzahl der Instanzen in den beiden Gruppen.

Umfang der Bereitschaft

Ein Bereitschaftsbereich identifiziert die Gruppierung von Ressourcen, die eine bestimmte Bereitschaftsprüfung umfasst. Der Umfang einer Bereitschaftsprüfung kann eine Wiederherstellungsgruppe (d. h. global für die gesamte Anwendung) oder eine Zelle (d. h. eine Region oder Availability Zone) sein. Bei einer Ressource, bei der es sich um eine globale Ressource für ARC handelt, legen Sie den Bereitschaftsbereich auf die Ebene der Wiederherstellungsgruppe oder der globalen Ressource fest. Beispielsweise ist eine Route 53-Zustandsprüfung eine globale Ressource in ARC, da sie nicht spezifisch für eine Region oder Availability Zone ist.

Daten- und Kontrollebenen für die Bereitschaftsprüfung

Denken Sie bei der Planung von Failover und Disaster Recovery darüber nach, wie robust Ihre Failover-Mechanismen sind. Es wird empfohlen, sicherzustellen, dass die Mechanismen,

auf die Sie beim Failover angewiesen sind, hochverfügbar sind, sodass Sie sie bei Bedarf in einem Notfallszenario verwenden können. In der Regel sollten Sie, wann immer möglich, Datenebenenfunktionen für Ihre Mechanismen verwenden, um die größtmögliche Zuverlässigkeit und Fehlertoleranz zu gewährleisten. Vor diesem Hintergrund ist es wichtig zu verstehen, wie die Funktionalität eines Dienstes zwischen Steuerungsebenen und Datenebenen aufgeteilt ist und wann Sie sich darauf verlassen können, dass die Datenebene eines Dienstes extrem zuverlässig ist.

Wie bei den meisten AWS Diensten wird die Funktionalität für die Bereitschaftsprüfung durch Steuerungsebenen und Datenebenen unterstützt. Beide sind zwar auf Zuverlässigkeit ausgelegt, eine Kontrollebene ist jedoch für die Datenkonsistenz optimiert, während eine Datenebene für die Verfügbarkeit optimiert ist. Eine Datenebene ist auf Ausfallsicherheit ausgelegt, sodass sie die Verfügbarkeit auch bei Störungen aufrechterhalten kann, wenn eine Kontrollebene möglicherweise nicht verfügbar ist.

Im Allgemeinen ermöglicht Ihnen eine Kontrollebene grundlegende Verwaltungsfunktionen wie das Erstellen, Aktualisieren und Löschen von Ressourcen im Service. Eine Datenebene stellt die Kernfunktionalität eines Dienstes bereit.

Für die Prüfung der Eignung gibt es eine einzige API, die Recovery Readiness API, sowohl für die Steuerungsebene als auch für die Datenebene. Bereitschaftsprüfungen und Bereitschaftsressourcen gibt es nur in der Region USA West (Oregon) (us-west-2). Die Kontrollebene und die Datenebene für die Bereitschaftsprüfung sind zuverlässig, aber nicht hochverfügbar.

Weitere Informationen zu Datenebenen, Kontrollebenen und dazu, wie Services AWS entwickelt werden, um Hochverfügbarkeitsziele zu erreichen, finden Sie im paper Statische Stabilität mithilfe von Availability Zones in der Amazon Builders' Library.

Tagging für die Bereitschaftsprüfung im Amazon Application Recovery Controller (ARC)

Tags sind Wörter oder Ausdrücke (Metadaten), die Sie verwenden, um Ihre AWS Ressourcen zu identifizieren und zu organisieren. Sie können jeder Ressource mehrere Tags hinzufügen, und jedes Tag enthält einen Schlüssel und einen Wert, den Sie festlegen. Der Schlüssel könnte beispielsweise die Umwelt und der Wert die Produktion sein. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags durchsuchen und filtern.

Sie können die folgenden Ressourcen bei der Bereitschaftsprüfung in ARC taggen:

- Ressourcensätze

- Prüfungen der Bereitschaft

Tagging in ARC ist nur über die API verfügbar, z. B. mit der AWS CLI.

Im Folgenden finden Sie Beispiele für das Taggen bei der Bereitschaftsprüfung mithilfe von. AWS CLI

```
aws route53-recovery-readiness --region us-west-2 create-resource-
set --resource-set-name dynamodb_resource_set --resource-set-type
AWS::DynamoDB::Table --resources ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/PDXCell,ResourceArn=arn:aws:dynamodb:us-
west-2:111122223333:table/PDX_Table ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/IADCell,ResourceArn=arn:aws:dynamodb:us-
east-1:111122223333:table/IAD_Table --tags Stage=Prod
```

```
aws route53-recovery-readiness --region us-west-2 create-readiness-
check --readiness-check-name dynamodb_readiness_check --resource-set-name
dynamodb_resource_set --tags Stage=Prod
```

Weitere Informationen finden Sie TagResourceim Recovery Readiness API-Referenzhandbuch für Amazon Application Recovery Controller (ARC).

Preise für den Bereitschaftstest in ARC

Pro von Ihnen konfigurierter Bereitschaftsprüfung zahlen Sie stündliche Kosten.

Detaillierte Preisinformationen für ARC und Preisbeispiele finden Sie unter ARC-Preise.

Richten Sie einen stabilen Wiederherstellungsprozess für Ihre Anwendung ein

Um Amazon Application Recovery Controller (ARC) mit AWS Anwendungen zu verwenden, die sich in mehreren AWS Regionen befinden, müssen Sie Richtlinien befolgen, um Ihre Anwendungen so einzurichten, dass sie ausfallsicher sind, sodass Sie die Wiederherstellungsbereitschaft effektiv unterstützen können. Anschließend können Sie Bereitschaftsprüfungen für Ihre Anwendung erstellen und Routingkontrollen einrichten, um den Datenverkehr für ein Failover umzuleiten. Sie können sich auch die Empfehlungen von ARC zur Architektur Ihrer Anwendung ansehen, mit der die Ausfallsicherheit verbessert werden kann.

> **Note**
>
> Wenn Sie eine Anwendung haben, die in Availability Zones isoliert ist, sollten Sie die Verwendung von Zonal Shift oder Zonal Autoshift für die Failover-Wiederherstellung in Betracht ziehen. Es ist keine Einrichtung erforderlich, um Zonal Shift oder Zonal Autoshift zu verwenden, um Anwendungen nach Beeinträchtigungen in der Availability Zone zuverlässig wiederherzustellen.
> Um den Traffic von einer Availability Zone für Load Balancer-Ressourcen weg zu verlagern, starten Sie eine Zonenverschiebung in der ARC-Konsole oder in der Elastic Load Balancing Balancing-Konsole. Oder Sie können das AWS SDK AWS Command Line Interface oder mit Zonal Shift-API-Aktionen verwenden. Weitere Informationen finden Sie unter Zonenverschiebung in ARC.

Weitere Informationen zu den ersten Schritten mit robusten Failover-Konfigurationen finden Sie unter. Erste Schritte mit der Wiederherstellung mehrerer Regionen in Amazon Application Recovery Controller (ARC)

Bewährte Methoden für die Prüfung der Eignung in ARC

Wir empfehlen die folgenden bewährten Methoden für die Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC).

Fügen Sie Benachrichtigungen für Änderungen des Bereitschaftsstatus hinzu

Legen Sie in Amazon eine Regel fest EventBridge , nach der eine Benachrichtigung gesendet wird, wenn sich der Status einer Bereitschaftsprüfung ändert, z. B. von `READY` zu`NOT READY`. Wenn Sie eine Benachrichtigung erhalten, können Sie das Problem untersuchen und beheben, um sicherzustellen, dass Ihre Anwendung und Ihre Ressourcen für den erwarteten Failover bereit sind.

Sie können EventBridge Regeln festlegen, um Benachrichtigungen für verschiedene Statusänderungen der Bereitschaftsprüfung zu senden, z. B. für Ihre Wiederherstellungsgruppe (für Ihre Anwendung), für eine Zelle (z. B. eine AWS Region) oder für eine Bereitschaftsprüfung für eine Ressourcengruppe.

Weitere Informationen finden Sie unter Bereitschaftsprüfung in ARC mit Amazon verwenden EventBridge.

API-Operationen zur Bereitschaftsprüfung

In der folgenden Tabelle sind ARC-Operationen aufgeführt, die Sie zur Überprüfung der Wiederherstellungsbereitschaft (Readiness Check) verwenden können, sowie Links zur entsprechenden Dokumentation.

Beispiele für die Verwendung gängiger API-Operationen zur Wiederherstellung in Verbindung mit dem AWS Command Line Interface finden Sie unter Beispiele für die Verwendung von API-Vorgängen zur ARC-Bereitschaftsprüfung mit dem AWS CLI.

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Erstellen Sie eine Zelle	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe CreateCell
Hol dir eine Zelle	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe GetCell
Lösche eine Zelle	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe DeleteCell
Eine Zelle aktualisieren	N/A	Siehe UpdateCell
Zellen für ein Konto auflisten	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe ListCells
Erstellen Sie eine Wiederherstellungsgruppe	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe CreateRecoveryGroup
Holen Sie sich eine Wiederherstellungsgruppe	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe GetRecoveryGroup

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Aktualisieren Sie eine Wiederherstellungsgruppe	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe UpdateRecoveryGroup
Löschen Sie eine Wiederherstellungsgruppe	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe DeleteRecoveryGroup
Wiederherstellungsgruppen auflisten	Siehe Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC	Siehe ListRecoveryGroups
Erstellen Sie einen Ressourcensatz	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe CreateResourceSet
Holen Sie sich ein Ressourceset	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe GetResourceSet
Aktualisieren Sie einen Ressourcensatz	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe UpdateResourceSet
Löschen Sie einen Ressourcensatz	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe DeleteResourceSet
Ressourcensätze auflisten	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe ListResourceSets
Erstellen Sie eine Bereitschaftsprüfung	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe CreateReadinessCheck

Aktion	Verwenden der ARC-Konsole	Verwendung der ARC-API
Holen Sie sich einen Bereitschaftscheck	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe GetReadinessCheck
Aktualisieren Sie eine Bereitschaftsprüfung	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe UpdateReadinessCheck
Löschen Sie eine Bereitschaftsprüfung	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe DeleteReadinessCheck
Führen Sie Bereitschaftsprüfungen auf	Siehe Bereitschaftsprüfungen in ARC erstellen und aktualisieren	Siehe ListReadinessChecks
Führen Sie die Bereitschaftsregeln auf	Siehe Beschreibungen der Bereitschaftsregeln in ARC	Siehe ListRules
Überprüfen Sie den Status einer gesamten Bereitschaftsprüfung	Siehe Überwachung des Bereitschaftsstatus in ARC	Siehe GetReadinessCheckStatus
Überprüfen Sie den Status einer Ressource	Siehe Überwachung des Bereitschaftsstatus in ARC	Siehe GetReadinessCheckResourceStatus
Überprüfen Sie den Status einer Zelle	Siehe Überwachung des Bereitschaftsstatus in ARC	Siehe GetCellReadinessSummary
Überprüfen Sie den Status einer Wiederherstellungsgruppe	Siehe Überwachung des Bereitschaftsstatus in ARC	Siehe GetRecoveryGroupReadinessSummary

Beispiele für die Verwendung von API-Vorgängen zur ARC-Bereitschaftsprüfung mit dem AWS CLI

In diesem Abschnitt werden einfache Anwendungsbeispiele vorgestellt, bei denen die Funktionen AWS Command Line Interface zur Prüfung der Bereitschaft von Amazon Application Recovery Controller (ARC) mithilfe von API-Vorgängen verwendet werden. Die Beispiele sollen Ihnen helfen, ein grundlegendes Verständnis dafür zu entwickeln, wie Sie mit Funktionen zur Bereitschaftsprüfung mithilfe der CLI arbeiten können.

Überprüfung der Verfügbarkeit bei ARC-Audits auf Diskrepanzen bei den Ressourcen in Ihren Anwendungsreplikaten. Um Bereitschaftsprüfungen für Ihre Anwendung einzurichten, müssen Sie Ihre Anwendungsressourcen in ARC-Zellen einrichten — oder modellieren —, die den Replikaten entsprechen, die Sie für Ihre Anwendung erstellt haben. Anschließend richten Sie Bereitschaftsprüfungen ein, mit denen diese Replikate geprüft werden, sodass Sie kontinuierlich sicherstellen können, dass Ihr Standby-Anwendungsreplikat und die zugehörigen Ressourcen mit Ihrem Produktionsreplikat übereinstimmen

Schauen wir uns einen einfachen Fall an, in dem Sie eine Anwendung mit dem Namen haben Simple-Service das derzeit in der Region USA Ost (Nord-Virginia) (US-East-1) läuft. Sie haben auch eine Bereitschaftskopie der Anwendung in der Region USA West (Oregon) (us-west-2). In diesem Beispiel konfigurieren wir Bereitschaftsprüfungen, um diese beiden Versionen der Anwendung zu vergleichen. Auf diese Weise können wir sicherstellen, dass die Standby-Region USA West (Oregon) bereit ist, Datenverkehr zu empfangen, falls dies in einem Failover-Szenario erforderlich ist.

Weitere Informationen zur Verwendung von finden Sie in der AWS CLI Befehlsreferenz. AWS CLI Eine Liste der Readiness-API-Aktionen und Links zu weiteren Informationen finden Sie unter API-Operationen zur Bereitschaftsprüfung.

Die Zellen in ARC stellen Fehlergrenzen dar (wie Availability Zones oder Regionen) und werden in Wiederherstellungsgruppen zusammengefasst. Eine Wiederherstellungsgruppe steht für eine Anwendung, für die Sie die Failover-Bereitschaft überprüfen möchten. Weitere Informationen zu den Komponenten der Bereitschaftsprüfung finden Sie unterKomponenten der Bereitschaftsprüfung .

> **Note**
>
> ARC ist ein globaler Dienst, der mehrere Endpunkte unterstützt, AWS-Regionen aber Sie müssen in den meisten ARC-CLI-Befehlen die Region USA West (Oregon`--region us-`

`west-2`) angeben (d. h. den Parameter angeben). Zum Beispiel, um Ressourcen wie Wiederherstellungsgruppen oder Bereitschaftsprüfungen zu erstellen.

In unserem Anwendungsbeispiel erstellen wir zunächst eine Zelle für jede Region, in der wir über Ressourcen verfügen. Dann erstellen wir eine Wiederherstellungsgruppe und schließen dann die Einrichtung für eine Eignungsprüfung ab.

1. Zellen erstellen

1a. Erstellen Sie eine US-East-1-Zelle.

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name east-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
    "CellName": "east-cell",
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1b. Erstellen Sie eine US-West-1-Zelle.

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name west-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell",
    "CellName": "west-cell",
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1c. Jetzt haben wir zwei Zellen. Sie können überprüfen, ob sie existieren, indem Sie die `list-cells` API aufrufen.

```
aws route53-recovery-readiness --region us-west-2 list-cells
```

```
{
    "Cells": [
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell",
            "CellName": "east-cell",
            "Cells": [],
            "ParentReadinessScopes": [],
            "Tags": {}
        },
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell",
            "CellName": "west-cell"
            "Cells": [],
            "ParentReadinessScopes": [],
            "Tags": {}
        }
    ]
}
```

2. Erstellen Sie eine Wiederherstellungsgruppe

Wiederherstellungsgruppen sind die wichtigste Ressource für die Wiederherstellungsbereitschaft in ARC. Eine Wiederherstellungsgruppe stellt eine Anwendung als Ganzes dar. In diesem Schritt erstellen wir eine Wiederherstellungsgruppe, um eine Gesamtanwendung zu modellieren, und fügen dann die beiden von uns erstellten Zellen hinzu.

2a. Erstellen Sie eine Wiederherstellungsgruppe.

```
aws route53-recovery-readiness --region us-west-2 create-recovery-group \
    --recovery-group-name simple-service-recovery-group \
       --cells "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"\
       "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
```

```
{
    "Cells": [],
    "RecoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/simple-service-recovery-group",
    "RecoveryGroupName": "simple-service-recovery-group",
    "Tags": {}
```

```
}
```

2b. (Optional) Sie können überprüfen, ob Ihre Wiederherstellungsgruppe korrekt erstellt wurde, indem Sie die `list-recovery-groups` API aufrufen.

```
aws route53-recovery-readiness --region us-west-2 list-recovery-groups
```

```
{
    "RecoveryGroups": [
        {
            "Cells": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
            "RecoveryGroupArn": "arn:aws:route53-recovery-
readiness::111122223333:recovery-group/simple-service-recovery-group",
            "RecoveryGroupName": "simple-service-recovery-group",
            "Tags": {}
        }
    ]
}
```

Da wir nun ein Modell für unsere Anwendung haben, fügen wir die zu überwachenden Ressourcen hinzu. In ARC wird eine Gruppe von Ressourcen, die Sie überwachen möchten, als Ressourcensatz bezeichnet. Ressourcensätze enthalten Ressourcen, die alle vom gleichen Typ sind. Wir vergleichen die Ressourcen in einem Ressourcensatz miteinander, um festzustellen, ob eine Zelle für einen Failover bereit ist.

3. Erstellen Sie einen Ressourcensatz

Nehmen wir an, unser Simple-Service Die Anwendung ist in der Tat sehr einfach und verwendet nur DynamoDB-Tabellen. Es hat eine DynamoDB-Tabelle in us-east-1 und eine weitere in us-west-2. Ein Ressourcensatz enthält auch einen Bereitschaftsbereich, der die Zelle identifiziert, in der sich die einzelnen Ressourcen befinden.

3a. Erstellen Sie ein Ressourcenset, das unsere widerspiegelt Simple-Service Ressourcen der Anwendung.

```
aws route53-recovery-readiness --region us-west-2 create-resource-set \
    --resource-set-name ImportantInformationTables \
    --resource-set-type AWS::DynamoDB::Table \
```

```
    --resources
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
west-cell"
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
east-cell"
```

```
{
    "ResourceSetArn": "arn:aws:route53-recovery-readiness::111122223333:resource-set/
sample-resource-set",
    "ResourceSetName": "ImportantInformationTables",
    "Resources": [
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
        }
    ],
    "Tags": {}
}
```

3b. (Optional) Sie können überprüfen, was im Ressourcensatz enthalten ist, indem Sie die `list-resource-sets` API aufrufen. Dies listet alle Ressourcensätze für ein AWS Konto auf. Hier können Sie sehen, dass wir nur den einen Ressourcensatz haben, den wir oben erstellt haben.

```
aws route53-recovery-readiness --region us-west-2 list-resource-sets
```

```
{
    "ResourceSets": [
        {
```

```
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
            ],
            "Tags": {}
        }
    ]
}{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-
readiness::&ExampleAWSAccountNo1;:cell/east-cell"
                    ],
```

```
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
            ],
            "Tags": {}
        }
    ]
}
```

Jetzt haben wir die Zellen, die Wiederherstellungsgruppe und den Ressourcensatz erstellt, um das zu modellieren Simple-Service Anwendung in ARC. Als Nächstes richten wir Bereitschaftsprüfungen ein, um zu überwachen, ob die Ressourcen für einen Failover bereit sind.

4. Erstellen Sie eine Bereitschaftsprüfung

Bei einer Bereitschaftsprüfung werden auf jede Ressource in der Ressourcengruppe, die mit der Prüfung verknüpft ist, eine Reihe von Regeln angewendet. Die Regeln sind für jeden Ressourcentyp spezifisch. Das heißt, es gibt unterschiedliche Regeln für `AWS::DynamoDB::TableAWS::EC2::Instance`, usw. Regeln prüfen eine Vielzahl von Dimensionen für eine Ressource, darunter Konfiguration, Kapazität (sofern verfügbar und zutreffend), Grenzwerte (sofern verfügbar und zutreffend) und Routing-Konfigurationen.

> **Note**
>
> Um zu sehen, welche Regeln bei einer Eignungsprüfung auf eine Ressource angewendet werden, können Sie die `get-readiness-check-resource-status` API verwenden, wie in Schritt 5 beschrieben. Eine Liste aller Bereitschaftsregeln in ARC finden Sie unter `list-rules` oder unterBeschreibungen der Bereitschaftsregeln in ARC. ARC verfügt über einen bestimmten Satz von Regeln, die für jeden Ressourcentyp ausgeführt werden. Sie können derzeit nicht angepasst werden.

4a. Erstellen Sie eine Eignungsprüfung für den Ressourcensatz, ImportantInformationTables.

```
aws route53-recovery-readiness --region us-west-2 create-readiness-check \
    --readiness-check-name ImportantInformationTableCheck --resource-set-name
 ImportantInformationTables
```

```
{
```

```
    "ReadinessCheckArn": "arn:aws:route53-recovery-readiness::111122223333:readiness-
check/ImportantInformationTableCheck",
    "ReadinessCheckName": "ImportantInformationTableCheck",
    "ResourceSet": "ImportantInformationTables",
    "Tags": {}
}
```

4b. (Optional) Führen Sie die `list-readiness-checks` API aus, um zu überprüfen, ob die Bereitschaftsprüfung erfolgreich erstellt wurde. Diese API zeigt alle Bereitschaftsprüfungen in einem Konto an.

```
aws route53-recovery-readiness --region us-west-2 list-readiness-checks
```

```
{
    "ReadinessChecks": [
        {
            "ReadinessCheckArn": "arn:aws:route53-recovery-
readiness::111122223333:readiness-check/ImportantInformationTableCheck",
            "ReadinessCheckName": "ImportantInformationTableCheck",
            "ResourceSet": "ImportantInformationTables",
            "Tags": {}
        }
    ]
}
```

5. Überwachen Sie die Bereitschaftsprüfungen

Nachdem wir die Anwendung modelliert und eine Eignungsprüfung hinzugefügt haben, sind wir bereit, die Ressourcen zu überwachen. Sie können die Bereitschaft Ihrer Anwendung auf vier Ebenen modellieren: der Bereitschaftsprüfungsebene (eine Gruppe von Ressourcen), der Ebene einzelner Ressourcen, der Zellebene (alle Ressourcen in einer Availability Zone oder Region) und der Ebene der Wiederherstellungsgruppe (die Anwendung als Ganzes). Im Folgenden finden Sie Befehle zum Abrufen der einzelnen Typen von Bereitschaftsstatus.

5a. Sehen Sie sich den Status Ihrer Bereitschaftsprüfung an.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status\
    --readiness-check-name ImportantInformationTableCheck
```

```
{
```

```
    "Readiness": "READY",
    "Resources": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast2"
    ]
}
```

5b. Sehen Sie sich den detaillierten Bereitschaftsstatus einer einzelnen Ressource in einer Bereitschaftsprüfung an, einschließlich des Status jeder geprüften Regel.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-resource-status \
    --readiness-check-name ImportantInformationTableCheck \
    --resource-identifier "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
```

```
{"Readiness": "READY",
    "Rules": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoTableStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoPeakRcuWcu"
```

```
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsConfig"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoReplicationLatency"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoAutoScalingConfiguration"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoLimits"
        }
    ]
```

```
}
```

5c. Sehen Sie sich die allgemeine Bereitschaft für eine Zelle an.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary \
    --cell-name west-cell
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

5d. Prüfen Sie abschließend, ob Ihre Anwendung auf oberster Ebene bereit ist, und zwar auf Ebene der Wiederherstellungsgruppe.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary
 \
    --recovery-group-name simple-service-recovery-group
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

Arbeiten mit Wiederherstellungsgruppen und Bereitschaftsprüfungen

In diesem Abschnitt werden Verfahren für Wiederherstellungsgruppen und Bereitschaftsprüfungen beschrieben und beschrieben, einschließlich der Erstellung, Aktualisierung und Löschung dieser Ressourcen.

Erstellen, Aktualisieren und Löschen von Wiederherstellungsgruppen in ARC

Eine Wiederherstellungsgruppe steht für Ihre Anwendung in Amazon Application Recovery Controller (ARC). Sie besteht in der Regel aus zwei oder mehr Zellen, die in Bezug auf Ressourcen und Funktionalität voneinander repliziert sind, sodass Sie ein Failover von einer zur anderen durchführen können. Jede Zelle enthält die Amazon-Ressourcennamen (ARNs) für die aktiven Ressourcen für eine AWS Region oder Availability Zone. Bei den Ressourcen kann es sich um einen Elastic Load Balancing Load Balancer, eine Auto Scaling Scaling-Gruppe oder andere Ressourcen handeln. Eine entsprechende Zelle, die eine andere Zone oder Region darstellt, verfügt über Standby-Ressourcen desselben Typs, die sich in Ihrer aktiven Zelle befinden — einen Load Balancer, eine Auto Scaling Scaling-Gruppe usw.

Eine Zelle steht für Replikate Ihrer Anwendung. Mithilfe von Bereitschaftsprüfungen in ARC können Sie feststellen, ob Ihre Anwendung für einen Failover von einem Replikat auf ein anderes bereit ist. Sie sollten jedoch auf der Grundlage Ihrer Überwachungs- und Integritätsprüfungssysteme entscheiden, ob ein Failaway oder ein Failaway zu einem Replikat durchgeführt werden soll, und Bereitschaftsprüfungen als ergänzenden Service für diese Systeme in Betracht ziehen.

Readiness Checks prüfen Ressourcen, um anhand einer Reihe von vordefinierten Regeln für diesen Ressourcentyp festzustellen, ob sie bereit sind. Nachdem Sie Ihre Wiederherstellungsgruppe mit den Replikaten erstellt haben, fügen Sie ARC-Bereitschaftsprüfungen für die Ressourcen in Ihrer Anwendung hinzu, sodass ARC sicherstellen kann, dass die Replikate im Laufe der Zeit dieselbe Einrichtung und Konfiguration haben.

Themen

- Wiederherstellungsgruppen erstellen
- Wiederherstellungsgruppen und -zellen aktualisieren und löschen

Wiederherstellungsgruppen erstellen

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Wiederherstellungsgruppe auf der ARC-Konsole erstellen. Weitere Informationen zur Verwendung von Recovery Readiness API-Vorgängen mit Amazon Application Recovery Controller (ARC) finden Sie unter API-Operationen zur Bereitschaftsprüfung.

Um eine Wiederherstellungsgruppe zu erstellen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Readiness Check.
3. Wählen Sie auf der Seite „Recovery Readiness“ die Option Create und anschließend eine Recovery-Gruppe aus.
4. Geben Sie einen Namen für Ihre Wiederherstellungsgruppe ein und wählen Sie dann Weiter.
5. Wählen Sie Zellen erstellen und dann Zelle hinzufügen aus.
6. Geben Sie einen Namen für die Zelle ein. Wenn Sie beispielsweise ein Anwendungsreplikat in US West (Nordkalifornien) haben, könnten Sie eine Zelle mit dem Namen `MyApp-us-west-1` hinzufügen.
7. Wählen Sie Zelle hinzufügen und fügen Sie einen Namen für eine zweite Zelle hinzu. Wenn Sie beispielsweise ein Replikat in USA East (Ohio) haben, könnten Sie eine Zelle mit dem Namen `MyApp-us-east-2` hinzufügen.
8. Wenn Sie verschachtelte Zellen (Replikate in Availability Zones innerhalb von Regionen) hinzufügen möchten, wählen Sie Aktion und dann Verschachtelte Zelle hinzufügen aus, und geben Sie dann einen Namen ein.
9. Wenn Sie alle Zellen und verschachtelten Zellen für Ihre Anwendungsreplikate hinzugefügt haben, wählen Sie Weiter aus.
10. Überprüfen Sie Ihre Wiederherstellungsgruppe und wählen Sie dann Create Recovery Group aus.

Wiederherstellungsgruppen und -zellen aktualisieren und löschen

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Wiederherstellungsgruppe aktualisieren und löschen und eine Zelle auf der ARC-Konsole löschen. Weitere Informationen zur Verwendung von Recovery Readiness API-Vorgängen mit Amazon Application Recovery Controller (ARC) finden Sie unter API-Operationen zur Bereitschaftsprüfung.

Um eine Wiederherstellungsgruppe zu aktualisieren oder zu löschen oder eine Zelle zu löschen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Readiness Check.

3. Wählen Sie auf der Seite „Wiederherstellungsbereitschaft“ eine Wiederherstellungsgruppe aus.
4. Um mit einer Wiederherstellungsgruppe zu arbeiten, wählen Sie Aktion und dann Wiederherstellungsgruppe bearbeiten oder Wiederherstellungsgruppe löschen.
5. Wenn Sie eine Wiederherstellungsgruppe bearbeiten, können Sie Zellen oder verschachtelte Zellen hinzufügen oder entfernen.
   - Um eine Zelle hinzuzufügen, wählen Sie Zelle hinzufügen.
   - Um eine Zelle zu entfernen, wählen Sie unter der Aktionsbeschriftung neben der Zelle die Option Zelle löschen aus.

Bereitschaftsprüfungen in ARC erstellen und aktualisieren

Dieser Abschnitt enthält Verfahren für Bereitschaftsprüfungen und Ressourcensätze, einschließlich der Erstellung, Aktualisierung und Löschung dieser Ressourcen.

Eine Bereitschaftsprüfung erstellen und aktualisieren

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Bereitschaftsprüfung auf der ARC-Konsole erstellen. Weitere Informationen zur Verwendung von Recovery Readiness API-Vorgängen mit Amazon Application Recovery Controller (ARC) finden Sie unter API-Operationen zur Bereitschaftsprüfung.

Um eine Bereitschaftsprüfung zu aktualisieren, können Sie den Ressourcensatz für die Bereitschaftsprüfung bearbeiten, Ressourcen hinzufügen oder entfernen oder den Bereitschaftsbereich für eine Ressource ändern.

Um eine Bereitschaftsprüfung zu erstellen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Readiness Check.
3. Wählen Sie auf der Bereitschaftsseite die Option Erstellen und anschließend eine Bereitschaftsprüfung aus.
4. Geben Sie einen Namen für Ihre Bereitschaftsprüfung ein, wählen Sie den Ressourcentyp aus, den Sie überprüfen möchten, und klicken Sie dann auf Weiter.

5. Fügen Sie einen Ressourcensatz für Ihre Eignungsprüfung hinzu. Ein Ressourcensatz ist eine Gruppe von Ressourcen desselben Typs in verschiedenen Replikaten. Wählen Sie eine der folgenden Optionen aus:

   - Erstellen Sie eine Eignungsprüfung mit Ressourcen in einem Ressourcensatz, den Sie bereits erstellt haben.
   - Erstellen Sie einen neuen Ressourcensatz.

   Wenn Sie einen neuen Ressourcensatz erstellen möchten, geben Sie einen Namen dafür ein und klicken Sie auf Hinzufügen.

6. Kopieren Sie die Amazon-Ressourcennamen (ARNs) nacheinander für jede Ressource, die Sie in die Gruppe aufnehmen möchten, und fügen Sie sie ein, und wählen Sie dann Weiter.

   > **Tip**
   >
   > Beispiele und weitere Informationen zum ARN-Format, das ARC für jeden Ressourcentyp erwartet, finden Sie unterRessourcentypen und ARN-Formate in ARC.

7. Wenn Sie möchten, können Sie sich die Bereitschaftsregeln ansehen, die verwendet werden, wenn ARC den Ressourcentyp überprüft, den Sie in diese Bereitschaftsprüfung aufgenommen haben. Wählen Sie anschließend Weiter.

8. (Optional) Wählen Sie unter Name der Wiederherstellungsgruppe eine Wiederherstellungsgruppe aus, der die Bereitschaftsprüfung zugeordnet werden soll, und wählen Sie dann für jeden Ressourcen-ARN eine Zelle (Region oder Availability Zone) aus dem Drop-down-Menü aus, in dem sich die Ressource befindet. Wenn es sich um eine Ressource auf Anwendungsebene handelt, z. B. eine DNS-Routing-Richtlinie, wählen Sie globale Ressource (keine Zelle) aus.

   Dies gibt die Bereitschaftsbereiche für die Ressourcen an, die bei der Bereitschaftsprüfung berücksichtigt werden.

   > **Important**
   >
   > Dieser Schritt ist zwar optional, allerdings müssen Bereitschaftsbereiche hinzugefügt werden, um eine Zusammenfassung der Bereitschaftsinformationen für Ihre Wiederherstellungsgruppe und Ihre Zellen zu erhalten. Wenn Sie diesen Schritt überspringen und die Bereitschaftsprüfung nicht mit den Ressourcen Ihrer

Wiederherstellungsgruppe verknüpfen, indem Sie hier Bereitschaftsbereiche auswählen, kann ARC keine zusammenfassenden Informationen zur Bereitschaft für die Wiederherstellungsgruppe oder -zellen zurückgeben.

9. Wählen Sie Weiter.
10. Überprüfen Sie die Informationen auf der Bestätigungsseite und wählen Sie dann Bereitschaftsprüfung erstellen aus.

Um eine Bereitschaftsprüfung zu löschen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Readiness Check.
3. Wählen Sie eine Bereitschaftsprüfung und wählen Sie unter Aktionen die Option Löschen aus.

Ressourcensätze erstellen und bearbeiten

In der Regel erstellen Sie einen Ressourcensatz im Rahmen einer Eignungsprüfung, aber Sie können einen Ressourcensatz auch separat erstellen. Sie können eine Ressourcengruppe auch bearbeiten, um Ressourcen hinzuzufügen oder zu entfernen. In den Schritten in diesem Abschnitt wird erklärt, wie Sie einen Ressourcensatz auf der ARC-Konsole erstellen oder bearbeiten. Weitere Informationen zur Verwendung von Recovery Readiness API-Vorgängen mit Amazon Application Recovery Controller (ARC) finden Sie unter API-Operationen zur Bereitschaftsprüfung.

Um einen Ressourcensatz zu erstellen

1. Öffnen Sie die Route 53-Konsole zu https://console.aws.amazon.com/route53/Hause.
2. Wählen Sie unter Application Recovery Controller die Option Resource Sets aus.
3. Wählen Sie Create (Erstellen) aus.
4. Geben Sie einen Namen für den Ressourcensatz ein und wählen Sie dann den Ressourcentyp aus, der in den Satz aufgenommen werden soll.
5. Wählen Sie Hinzufügen und geben Sie dann den Amazon-Ressourcennamen (ARN) für die Ressource ein, die dem Set hinzugefügt werden soll.
6. Wenn Sie mit dem Hinzufügen von Ressourcen fertig sind, wählen Sie Create Resource Set aus.

Um einen Ressourcensatz zu bearbeiten

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Readiness Check.
3. Wählen Sie unter Ressourcensets die Option Aktion und dann Bearbeiten aus.
4. Führen Sie eine der folgenden Aktionen aus:
   - Um eine Ressource aus dem Satz zu entfernen, wählen Sie Entfernen aus.
   - Um dem Set eine Ressource hinzuzufügen, wählen Sie Hinzufügen und geben Sie dann den Amazon-Ressourcennamen (ARN) für die Ressource ein.
5. Sie können auch den Bereitschaftsbereich für die Ressource bearbeiten, um die Ressource einer anderen Zelle für die Bereitschaftsprüfung zuzuordnen.
6. Wählen Sie Save (Speichern) aus.

Überwachung des Bereitschaftsstatus in ARC

Sie können die Bereitschaft Ihrer Anwendung in Amazon Application Recovery Controller (ARC) auf den folgenden Ebenen überprüfen:

- Die Stufe der Bereitschaftsprüfung für die Ressourcen in einem Ressourcensatz
- Die individuelle Ressourcenebene
- Die Zellebene (Anwendungsreplikat) für alle Ressourcen in einer Availability Zone oder Region AWS
- Die Wiederherstellungsgruppenebene für die gesamte Anwendung

Sie können über Änderungen des Bereitschaftsstatus benachrichtigt werden, oder Sie können Änderungen des Bereitschaftsstatus in der Route 53-Konsole oder mithilfe von ARC-CLI-Befehlen überwachen.

Benachrichtigung über den Bereitschaftsstatus

Sie können Amazon verwenden EventBridge , um ereignisgesteuerte Regeln einzurichten, um ARC-Ressourcen zu überwachen und Sie über Änderungen des Bereitschaftsstatus zu informieren. Weitere Informationen finden Sie unter Bereitschaftsprüfung in ARC mit Amazon verwenden EventBridge.

Überwachung des Bereitschaftsstatus in der ARC-Konsole

Das folgende Verfahren beschreibt, wie Sie die Wiederherstellungsbereitschaft in der überwachen AWS Management Console.

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Readiness Check.
3. Sehen Sie sich auf der Seite „Bereitschaft“ unter Wiederherstellungsgruppe den Bereitschaftsstatus der Wiederherstellungsgruppe für jede Wiederherstellungsgruppe (Anwendung) an.

   Sie können auch die Bereitschaft bestimmter Zellen oder einzelner Ressourcen einsehen.

Überwachung des Bereitschaftsstatus mithilfe von CLI-Befehlen

Dieser Abschnitt enthält Beispiele für AWS CLI Befehle, mit denen Sie den Bereitschaftsstatus Ihrer Anwendung und Ressourcen auf verschiedenen Ebenen anzeigen können.

Bereitschaft für einen Ressourcensatz

Der Status einer Bereitschaftsprüfung, die Sie für eine Ressourcengruppe (eine Gruppe von Ressourcen) erstellt haben.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName
```

Bereitschaft für eine einzelne Ressource

Um den Status einer einzelnen Ressource in einer Bereitschaftsprüfung abzurufen, einschließlich des Status jeder geprüften Bereitschaftsregel, geben Sie den Namen der Bereitschaftsprüfung und einen Ressourcen-ARN an. Zum Beispiel:

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName --resource-arn "arn:aws:dynamodb:us-west-2:111122223333:table/TableName"
```

Bereitschaft für eine Zelle

Der Status einer einzelnen Zelle, d. h. einer Region oder Availability Zone.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-
summary --cell-name CellName
```

Bereitschaft für eine Bewerbung

Der Status der gesamten Anwendung auf der Ebene der Wiederherstellungsgruppe.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-
readiness-summary --recovery-group-name RecoveryGroupName
```

Abrufen von Architekturempfehlungen in ARC

Wenn Sie über eine bestehende Anwendung verfügen, kann Amazon Application Recovery Controller (ARC) die Architektur Ihrer Anwendung und die Routing-Richtlinien bewerten, um Empfehlungen zur Änderung des Designs zur Verbesserung der Wiederherstellungsresistenz Ihrer Anwendung zu geben. Nachdem Sie in ARC eine Wiederherstellungsgruppe erstellt haben, die Ihre Anwendung repräsentiert, folgen Sie den Schritten in diesem Abschnitt, um Empfehlungen für die Architektur Ihrer Anwendung zu erhalten.

Wir empfehlen Ihnen, eine Zielressource für die DNS-Zielressource für Ihre Wiederherstellungsgruppe anzugeben, falls Sie noch keine angegeben haben, damit wir detailliertere Empfehlungen geben können. Wenn Sie zusätzliche Informationen angeben, kann ARC Ihnen bessere Empfehlungen geben. Wenn Sie beispielsweise einen Amazon Route 53-Ressourceneintrag oder einen Network Load Balancer als Zielressource eingeben, kann ARC Informationen darüber bereitstellen, ob Sie die optimale Anzahl von Zellen für Ihre Wiederherstellungsgruppe erstellt haben.

Beachten Sie Folgendes für DNS-Zielressourcen:

- Geben Sie nur einen Route 53-Ressourceneintrag oder einen Network Load Balancer für eine Zielressource an.
- Erstellen Sie nur eine DNS-Zielressource für jede Wiederherstellungsgruppe.
- Empfehlung: Erstellen Sie eine DNS-Zielressource für jede Zelle.
- Gruppieren Sie die DNS-Zielressourcen zu einem Ressourcensatz mit einer Eignungsprüfung.

Das folgende Verfahren erklärt, wie Sie DNS-Zielressourcen erstellen und Architekturempfehlungen für Ihre Anwendung abrufen.

Um Empfehlungen für die Aktualisierung Ihrer Architektur zu erhalten

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Readiness Check.
3. Wählen Sie unter Name der Wiederherstellungsgruppe die Wiederherstellungsgruppe aus, die Ihrer Anwendung entspricht.
4. Wählen Sie auf der Seite mit den Details der Wiederherstellungsgruppe im Menü Aktion die Option Architekturempfehlungen für diese Wiederherstellungsgruppe abrufen aus.
5. Wenn Sie noch keine Prüfung der Eignung für DNS-Zielressourcen erstellt haben, erstellen Sie eine, damit ARC Architekturempfehlungen geben kann. Wählen Sie Eine DNS-Zielressource erstellen aus.

   Weitere Informationen zu DNS-Zielressourcen finden Sie unterKomponenten der Bereitschaftsprüfung .
6. Um einen Ressourcensatz für eine DNS-Zielressource zu erstellen, erstellen Sie eine Bereitschaftsprüfung. Geben Sie einen Namen für die Bereitschaftsprüfung ein, und wählen Sie dann für den Typ der Bereitschaftsprüfung die DNS-Zielressource aus.
7. Geben Sie einen Namen für den Ressourcensatz ein.
8. Geben Sie die Attribute für Ihre Anwendung ein, darunter den DNS-Namen, den ARN der gehosteten Zone und die Datensatz-ID.

   > **Tip**
   >
   > Das ARN-Format für eine gehostete Zone ARN Sie unter ARN-Format für gehostete Zone inRessourcentypen und ARN-Formate in ARC.

   Optional, aber dringend empfohlen, wählen Sie Optionales Attribut hinzufügen und geben Sie einen Network Load Balancer Balancer-ARN oder den Route 53-Ressourceneintrag Ihrer Domain an.
9. (Optional) Wählen Sie in der Konfiguration der Wiederherstellungsgruppe eine Zelle für Ihre DNS-Zielressource aus, um den Bereitschaftsbereich festzulegen.
10. Wählen Sie Create Resource Set aus.

11. Wählen Sie auf der Seite mit den Details zur Wiederherstellungsgruppe die Option Architekturempfehlungen abrufen aus. ARC zeigt auf der Seite eine Reihe von Empfehlungen an.

Sehen Sie sich die Liste der Empfehlungen an. Anschließend können Sie entscheiden, ob und wie Sie Änderungen vornehmen möchten, um die Widerstandsfähigkeit Ihrer App bei der Wiederherstellung zu verbessern.

Kontoübergreifende Autorisierungen in ARC erstellen

Möglicherweise sind Ihre Ressourcen auf mehrere AWS Konten verteilt, was es schwierig machen kann, sich einen umfassenden Überblick über den Zustand Ihrer Anwendung zu verschaffen. Es kann auch schwierig sein, die Informationen zu erhalten, die für schnelle Entscheidungen erforderlich sind. Um diese Prüfung der Eignung in Amazon Application Recovery Controller (ARC) zu vereinfachen, können Sie die kontoübergreifende Autorisierung verwenden.

Die kontoübergreifende Autorisierung in ARC funktioniert mit der Funktion zur Prüfung der Eignung. Mit der kontoübergreifenden Autorisierung können Sie ein zentrales AWS Konto verwenden, um Ihre Ressourcen zu überwachen, die sich in mehreren AWS Konten befinden. In jedem Konto, das über Ressourcen verfügt, die Sie überwachen möchten, autorisieren Sie das zentrale Konto für den Zugriff auf diese Ressourcen. Anschließend kann das zentrale Konto Bereitschaftsprüfungen für die Ressourcen in allen Konten durchführen, und vom zentralen Konto aus können Sie die Bereitschaft für einen Failover überwachen.

> **Note**
>
> Die Einrichtung der kontoübergreifenden Autorisierung ist in der Konsole nicht verfügbar. Verwenden Sie stattdessen ARC-API-Operationen, um die kontoübergreifende Autorisierung einzurichten und damit zu arbeiten. Um Ihnen den Einstieg zu erleichtern, finden Sie in diesem Abschnitt AWS CLI Befehlsbeispiele.

Nehmen wir an, eine Anwendung hat ein Konto mit Ressourcen in der Region USA West (Oregon) (us-west-2), und es gibt auch ein Konto mit Ressourcen, die Sie in der Region USA Ost (Nord-Virginia) (us-east-1) überwachen möchten. ARC kann Ihnen den Zugriff auf die Überwachung beider Ressourcensätze von einem Konto, us-west-2, aus ermöglichen, indem Sie die kontoübergreifende Autorisierung verwenden.

Nehmen wir zum Beispiel an, Sie haben die folgenden Konten: AWS

- US-West-Konto: 999999999999
- Konto US-Ost: 111111111111

Im Konto us-east-1 (111111111111) können wir die kontoübergreifende Autorisierung aktivieren, um den Zugriff durch das US-West-2-Konto (99999999999999) zu ermöglichen, indem wir den Amazon-Ressourcennamen (ARN) für den (Root-) Benutzer im IAM-Konto us-west-2 angeben:. `arn:aws:iam::999999999999:root` Nachdem wir die Autorisierung erstellt haben, kann das us-west-2-Konto Ressourcen, die us-east-1 gehören, zu Ressourcensätzen hinzufügen und Bereitschaftsprüfungen erstellen, die für die Ressourcensätze ausgeführt werden.

Das folgende Beispiel veranschaulicht die Einrichtung der kontoübergreifenden Autorisierung für ein Konto. Sie müssen die kontenübergreifende Autorisierung für jedes weitere Konto aktivieren, das über AWS Ressourcen verfügt, die Sie in ARC hinzufügen und überwachen möchten.

> **Note**
>
> ARC ist ein globaler Dienst, der Endpunkte in mehreren AWS Regionen unterstützt, aber Sie müssen in den meisten ARC-CLI-Befehlen die Region USA West (Oregon`--region us-west-2`) angeben (d. h. den Parameter angeben).

Der folgende AWS CLI Befehl zeigt, wie Sie die kontoübergreifende Autorisierung für dieses Beispiel einrichten:

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-account \
    create-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

Gehen Sie wie folgt vor, um diese Autorisierung zu deaktivieren:

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-account \
    delete-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

Verwenden Sie den `list-cross-account-authorizations` Befehl, um ein bestimmtes Konto für alle Konten einzuchecken, für die Sie eine kontoübergreifende Autorisierung erteilt haben.

Beachten Sie, dass Sie derzeit nicht in die andere Richtung einchecken können. Das heißt, es gibt keinen API-Vorgang, den Sie mit einem Kontoprofil verwenden können, um alle Konten aufzulisten, für die dem Profil eine kontenübergreifende Autorisierung zum Hinzufügen und Überwachen von Ressourcen erteilt wurde.

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-account \
    list-cross-account-authorizations
```

```
{
    "CrossAccountAuthorizations": [
        "arn:aws:iam::999999999999:root"
    ]
}
```

Bereitschaftsregeln, Ressourcentypen und ARNS

Dieser Abschnitt enthält Referenzinformationen zu den Bereitschaftsregeln, Beschreibungen und unterstützten Ressourcentypen sowie zum Format für Amazon-Ressourcennamen (ARNs), das Sie für Ressourcensätze verwenden.

Beschreibungen der Bereitschaftsregeln in ARC

In diesem Abschnitt werden die Bereitschaftsregeln für alle Arten von Ressourcen beschrieben, die von Amazon Application Recovery Controller (ARC) unterstützt werden. Eine Liste der von ARC unterstützten Ressourcentypen finden Sie unterRessourcentypen und ARN-Formate in ARC.

Sie können die Beschreibungen der Bereitschaftsregeln auch auf der ARC-Konsole oder mithilfe einer API-Operation anzeigen, indem Sie wie folgt vorgehen:

- Gehen Sie wie folgt vor, um die Bereitschaftsregeln in der Konsole anzuzeigen:Bereitschaftsregeln auf der Konsole anzeigen.
- Informationen zum Anzeigen von Bereitschaftsregeln mithilfe der API finden Sie im ListRulesVorgang.

Themen

- Bereitschaftsregeln in ARC
- Bereitschaftsregeln auf der Konsole anzeigen

Bereitschaftsregeln in ARC

In diesem Abschnitt werden die Bereitschaftsregeln für jeden Ressourcentyp aufgeführt, der von ARC unterstützt wird.

Wenn Sie sich die Regelbeschreibungen ansehen, werden Sie feststellen, dass die meisten von ihnen die Begriffe „Prüft alle“ oder „Prüft alle“ enthalten. Weitere Informationen darüber, wie diese Begriffe erklären, wie eine Regel im Kontext einer Bereitschaftsprüfung funktioniert, und weitere Informationen dazu, wie ARC den Bereitschaftsstatus festlegt, finden Sie unter So bestimmen Bereitschaftsregeln den Bereitschaftsstatus.

Bereitschaftsregeln

ARC prüft Ressourcen anhand der folgenden Bereitschaftsregeln.

Stufen von Amazon API Gateway Version 1

- ApiGwV1ApiKeyCount: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass mit ihnen die gleiche Anzahl von API-Schlüsseln verknüpft ist.
- ApiGwV1ApiKeySource: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `API Key Source` haben.
- ApiGwV1BasePath: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie mit demselben Basispfad verknüpft sind.
- ApiGwV1BinaryMediaTypes: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie dieselben binären Medientypen unterstützen.
- ApiGwV1CacheClusterEnabled: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass entweder alle `Cache Cluster` aktiviert sind oder keine.
- ApiGwV1CacheClusterSize: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sie dieselben `Cache Cluster Size` haben. Wenn einer Wert einen höheren Wert hat, werden die anderen als NICHT BEREIT markiert.
- ApiGwV1CacheClusterStatus: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sich der im Status `Cache Cluster` AVAILABLE befindet.
- ApiGwV1DisableExecuteApiEndpoint: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass entweder alle `Execute API Endpoint` deaktiviert wurden oder keine.
- ApiGwV1DomainName: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie mit demselben Domainnamen verknüpft sind.
- ApiGwV1EndpointConfiguration: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sie mit einer Domain mit derselben Endpunktkonfiguration verknüpft sind.

- ApiGwV1EndpointDomainNameStatus: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass der Domainname, mit dem sie verknüpft sind, den Status AVAILABLE hat.
- ApiGwV1MethodSettings: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Method Settings` haben.
- ApiGwV1MutualTlsAuthentication: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Mutual TLS Authentication` haben.
- ApiGwV1Policy: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass entweder alle Richtlinien auf API-Ebene verwenden oder keine.
- ApiGwV1RegionalDomainName: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sie mit demselben regionalen Domainnamen verknüpft sind. Hinweis: Diese Regel hat keinen Einfluss auf den Bereitschaftsstatus.
- ApiGwV1ResourceMethodConfigs: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sie eine ähnliche Ressourcenhierarchie haben, einschließlich der zugehörigen Konfigurationen.
- ApiGwV1SecurityPolicy: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Security Policy` haben.
- ApiGwV1Quotas: Überprüft alle API Gateway Gateway-Gruppen, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Limits) entsprechen.
- ApiGwV1UsagePlans: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie `Usage Plans` mit derselben Konfiguration verknüpft sind.

Amazon API Gateway Version 2, Stufen

- ApiGwV2ApiKeySelectionExpression: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sie denselben Wert für `API Key Selection Expression` haben.
- ApiGwV2ApiMappingSelectionExpression: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `API Mapping Selection Expression` haben.
- ApiGwV2CorsConfiguration: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sie dieselbe CORS-bezogene Konfiguration haben.
- ApiGwV2DomainName: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie mit demselben Domainnamen verknüpft sind.
- ApiGwV2DomainNameStatus: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sich der Domainname im Status AVAILABLE befindet.
- ApiGwV2EndpointType: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Endpoint Type` haben.

- ApiGwV2Quotas: Überprüft alle API Gateway Gateway-Gruppen, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Limits) entsprechen.
- ApiGwV2MutualTlsAuthentication: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Mutual TLS Authentication` haben.
- ApiGwV2ProtocolType: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Protocol Type` haben.
- ApiGwV2RouteConfigs: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sie dieselbe Hierarchie von Routen mit derselben Konfiguration haben.
- ApiGwV2RouteSelectionExpression: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Route Selection Expression` haben.
- ApiGwV2RouteSettings: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Default Route Settings` haben.
- ApiGwV2SecurityPolicy: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Security Policy` haben.
- ApiGwV2StageVariables: Überprüft alle API-Gateway-Phasen, um sicherzustellen, dass sie alle dieselben Stufen haben `Stage Variables` wie die anderen Stufen.
- ApiGwV2ThrottlingBurstLimit: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Throttling Burst Limit` haben.
- ApiGwV2ThrottlingRateLimit: Überprüft alle API-Gateway-Stufen, um sicherzustellen, dass sie denselben Wert für `Throttling Rate Limit` haben.

Amazon Aurora Aurora-Cluster

- RdsClusterStatus: Prüft jeden Aurora-Cluster, um sicherzustellen, dass er den Status entweder `AVAILABLE` oder `BACKING-UP` hat.
- RdsEngineMode: Überprüft alle Aurora-Cluster, um sicherzustellen, dass sie denselben Wert für `Engine Mode` haben.
- RdsEngineVersion: Überprüft alle Aurora-Cluster, um sicherzustellen, dass sie denselben Wert für `Major Version` haben.
- RdsGlobalReplicaLag: Prüft jeden Aurora-Cluster, um sicherzustellen, dass er eine Zeit `Global Replica Lag` von weniger als 30 Sekunden hat.
- RdsNormalizedCapacity: Überprüft alle Aurora-Cluster, um sicherzustellen, dass sie eine normalisierte Kapazität haben, die innerhalb von 15% des Maximums im Ressourcensatz liegt.
- RdsInstanceType: Überprüft alle Aurora-Cluster, um sicherzustellen, dass sie dieselben Instance-Typen haben.

- RdsQuotas: Überprüft alle Aurora-Cluster, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Limits) entsprechen.

Auto-Scaling-Gruppen

- AsgMinSizeAndMaxSize: Überprüft alle Auto Scaling Scaling-Gruppen, um sicherzustellen, dass sie dieselbe minimale und maximale Gruppengröße haben.
- AsgAZCount: Überprüft alle Auto Scaling Scaling-Gruppen, um sicherzustellen, dass sie dieselbe Anzahl von Availability Zones haben.
- AsgInstanceTypes: Überprüft alle Auto Scaling Scaling-Gruppen, um sicherzustellen, dass sie dieselben Instance-Typen haben. Hinweis: Diese Regel hat keinen Einfluss auf den Bereitschaftsstatus.
- AsgInstanceSizes: Überprüft alle Auto Scaling Scaling-Gruppen, um sicherzustellen, dass sie die gleichen Instanzgrößen haben.
- AsgNormalizedCapacity: Überprüft alle Auto Scaling Scaling-Gruppen, um sicherzustellen, dass sie über eine normalisierte Kapazität verfügen, die innerhalb von 15% des Maximums im Ressourcensatz liegt.
- AsgQuotas: Überprüft alle Auto Scaling Scaling-Gruppen, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Limits) entsprechen.

CloudWatch Alarme

- CloudWatchAlarmState: Überprüft die CloudWatch Alarme, um sicherzustellen, dass sie sich nicht im `INSUFFICIENT_DATA` Zustand `ALARM` oder befinden.

Kunden-Gateways

- CustomerGatewayIpAddress: Überprüft alle Kunden-Gateways, um sicherzustellen, dass sie dieselbe IP-Adresse haben.
- CustomerGatewayState: Überprüft Kunden-Gateways, um sicherzustellen, dass sich jedes Gateway im richtigen Zustand befindet. `AVAILABLE`
- CustomerGatewayVPNType: Überprüft alle Kunden-Gateways, um sicherzustellen, dass sie denselben VPN-Typ haben.

DNS target resources

- DnsTargetResourceHostedZoneConfigurationRule: Überprüft alle DNS-Zielressourcen, um sicherzustellen, dass sie dieselbe Amazon Route 53-Hosting-Zonen-ID haben und dass nicht jede gehostete Zone privat ist. Hinweis: Diese Regel hat keinen Einfluss auf den Bereitschaftsstatus.

- DnsTargetResourceRecordSetConfigurationRule: Überprüft alle DNS-Zielressourcen, um sicherzustellen, dass sie dieselbe Gültigkeitsdauer (TTL) für den Ressourcendatensatz haben und dass sie kleiner oder gleich 300 TTLs sind.
- DnsTargetResourceRoutingRule: Prüft jede DNS-Zielressource, die einem Alias-Ressourcendatensatz zugeordnet ist, um sicherzustellen, dass der Datenverkehr an den DNS-Namen weitergeleitet wird, der auf der Zielressource konfiguriert ist. Hinweis: Diese Regel hat keinen Einfluss auf den Bereitschaftsstatus.
- DnsTargetResourceHealthCheckRule: Überprüft alle DNS-Zielressourcen, um sicherzustellen, dass Zustandsprüfungen gegebenenfalls ihren Ressourcendatensätzen zugeordnet werden und ansonsten nicht. Hinweis: Diese Regel hat keinen Einfluss auf den Bereitschaftsstatus.

Amazon-DynamoDB-Tabellen

- DynamoConfiguration: Prüft alle DynamoDB-Tabellen, um sicherzustellen, dass sie dieselben Schlüssel, Attribute, serverseitigen Verschlüsselungs- und Streams-Konfigurationen haben.
- DynamoTableStatus: Prüft jede DynamoDB-Tabelle, um sicherzustellen, dass sie den Status ACTIVE hat.
- DynamoCapacity: Prüft alle DynamoDB-Tabellen, um sicherzustellen, dass ihre bereitgestellten Lese- und Schreibkapazitäten innerhalb von 20% der maximalen Kapazitäten im Ressourcensatz liegen.
- DynamoPeakRcuWcu: Prüft jede DynamoDB-Tabelle, um sicherzustellen, dass sie einen ähnlichen Spitzenverkehr hatte wie die anderen Tabellen, um die bereitgestellte Kapazität sicherzustellen.
- DynamoGsiPeakRcuWcu: Prüft jede DynamoDB-Tabelle, um sicherzustellen, dass sie eine ähnliche maximale Lese- und Schreibkapazität wie die anderen Tabellen hatte, um die bereitgestellte Kapazität sicherzustellen.
- DynamoGsiConfig: Prüft alle DynamoDB-Tabellen mit globalen Sekundärindizes, um sicherzustellen, dass die Tabellen denselben Index, dasselbe Schlüsselschema und dieselbe Projektion verwenden.
- DynamoGsiStatus: Prüft alle DynamoDB-Tabellen mit globalen Sekundärindizes, um sicherzustellen, dass die globalen Sekundärindizes den Status ACTIVE haben.
- DynamoGsiCapacity: Prüft alle DynamoDB-Tabellen mit globalen Sekundärindizes, um sicherzustellen, dass die Tabellen GSI-Lesekapazitäten und GSI-Schreibkapazitäten innerhalb von 20% der maximalen Kapazitäten im Ressourcensatz bereitgestellt haben.
- DynamoReplicationLatency: Prüft alle DynamoDB-Tabellen, bei denen es sich um globale Tabellen handelt, um sicherzustellen, dass sie dieselbe Replikationslatenz haben.

- DynamoAutoScalingConfiguration: Prüft alle DynamoDB-Tabellen, für die Auto Scaling aktiviert ist, um sicherzustellen, dass sie dieselben minimalen, maximalen und Ziel-Lese- und Schreibkapazitäten haben.
- DynamoQuotas: Überprüft alle DynamoDB-Tabellen, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Grenzwerten) entsprechen.

Elastic Load Balancing (Classic Load Balancer)

- ElbV1CheckAzCount: Prüft jeden Classic Load Balancer, um sicherzustellen, dass er nur mit einer Availability Zone verbunden ist. Hinweis: Diese Regel hat keinen Einfluss auf den Bereitschaftsstatus.
- ElbV1AnyInstances: Überprüft alle Classic Load Balancer, um sicherzustellen, dass sie über mindestens eine EC2 Instanz verfügen.
- ElbV1AnyInstancesHealthy: Prüft alle Classic Load Balancer, um sicherzustellen, dass sie über mindestens eine fehlerfreie Instanz verfügen. EC2
- ElbV1Scheme: Prüft alle Classic Load Balancer, um sicherzustellen, dass sie über dasselbe Load Balancer-Schema verfügen.
- ElbV1HealthCheckThreshold: Prüft alle Classic Load Balancer, um sicherzustellen, dass sie denselben Schwellenwert für die Integritätsprüfung haben.
- ElbV1HealthCheckInterval: Prüft alle Classic Load Balancer, um sicherzustellen, dass sie denselben Wert für das Intervall für die Integritätsprüfung haben.
- ElbV1CrossZoneRoutingEnabled: Überprüft alle Classic Load Balancer, um sicherzustellen, dass sie denselben Wert für den zonenübergreifenden Load Balancing haben (AKTIVIERT oder DEAKTIVIERT).
- ElbV1AccessLogsEnabledAttribute: Überprüft alle Classic Load Balancer, um sicherzustellen, dass sie denselben Wert für Zugriffsprotokolle haben (AKTIVIERT oder DEAKTIVIERT).
- ElbV1ConnectionDrainingEnabledAttribute: Überprüft alle Classic Load Balancer, um sicherzustellen, dass sie den gleichen Wert für den Verbindungsabbau haben (ENABLED oder DISABLED).
- ElbV1ConnectionDrainingTimeoutAttribute: Überprüft alle Classic Load Balancer, um sicherzustellen, dass sie denselben Timeout-Wert für den Verbindungsabbau haben.
- ElbV1IdleTimeoutAttribute: Überprüft alle Classic Load Balancer, um sicherzustellen, dass sie denselben Wert für das Timeout im Leerlauf haben.
- ElbV1ProvisionedCapacityLcuCount: Überprüft alle Classic Load Balancer mit einer bereitgestellten LCU von mehr als 10, um sicherzustellen, dass sie sich innerhalb von 20% der am höchsten bereitgestellten LCU in der Ressourcengruppe befinden.

- ElbV1ProvisionedCapacityStatus: Prüft den Status der bereitgestellten Kapazität auf jedem Classic Load Balancer, um sicherzustellen, dass er nicht den Wert DISABLED oder PENDING hat.

Amazon-EBS-Volumes

- EbsVolumeEncryption: Prüft alle EBS Volumes, um sicherzustellen, dass sie denselben Verschlüsselungswert haben (AKTIVIERT oder DEAKTIVIERT).
- EbsVolumeEncryptionDefault: Prüft alle EBS Volumes, um sicherzustellen, dass sie standardmäßig denselben Verschlüsselungswert haben (AKTIVIERT oder DEAKTIVIERT).
- EbsVolumeIops: Prüft alle EBS Volumes, um sicherzustellen, dass sie dieselben Eingabe-/Ausgabeoperationen pro Sekunde (IOPS) haben.
- EbsVolumeKmsKeyId: Prüft alle EBS Volumen, um sicherzustellen, dass sie dieselbe AWS KMS Standardschlüssel-ID haben.
- EbsVolumeMultiAttach: Prüft alle EBS Volumes, um sicherzustellen, dass sie denselben Wert für Multi-Attach haben (AKTIVIERT oder DEAKTIVIERT).
- EbsVolumeQuotas: Prüft alle EBS Volumen, um sicherzustellen, dass sie den durch Service Quotas festgelegten Kontingenten (Limits) entsprechen.
- EbsVolumeSize: Prüft alle EBS Volumen, um sicherzustellen, dass sie dieselbe lesbare Größe haben.
- EbsVolumeState: Prüft alle EBS Volumes, um sicherzustellen, dass sie den gleichen Volumenstatus haben.
- EbsVolumeType: Prüft alle EBS Volumen, um sicherzustellen, dass sie denselben Datenträgertyp haben.

AWS Lambda Funktionen

- LambdaMemorySize: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie dieselbe Speichergröße haben. Wenn eine mehr Speicher hat, werden die anderen markiert. `NOT READY`
- LambdaFunctionTimeout: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie denselben Timeout-Wert haben. Wenn eine davon einen höheren Wert hat, werden die anderen markiert. `NOT READY`
- LambdaFunctionRuntime: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie alle dieselbe Laufzeit haben.

- LambdaFunctionReservedConcurrentExecutions: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie alle den gleichen Wert für haben. `Reserved Concurrent Executions` Wenn eine einen höheren Wert hat, werden die anderen markiert. `NOT READY`
- LambdaFunctionDeadLetterConfig: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie entweder alle eine `Dead Letter Config` definierte haben oder dass keine von ihnen eine definierte hat.
- LambdaFunctionProvisionedConcurrencyConfig: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie denselben Wert für haben. `Provisioned Concurrency`
- LambdaFunctionSecurityGroupCount: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie denselben Wert für haben. `Security Groups`
- LambdaFunctionSubnetIdCount: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie denselben Wert für haben. `Subnet Ids`
- LambdaFunctionEventSourceMappingMatch: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass alle ausgewählten `Event Source Mapping` Eigenschaften übereinstimmen.
- LambdaFunctionLimitsRule: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie den von Service Quotas verwalteten Quotas (Grenzwerten) entsprechen.

Network Load Balancer und Application Load Balancer

- ElbV2CheckAzCount: Prüft jeden Network Load Balancer, um sicherzustellen, dass er nur mit einer Availability Zone verbunden ist. Hinweis: Diese Regel hat keinen Einfluss auf den Bereitschaftsstatus.
- ElbV2TargetGroupsCanServeTraffic: Prüft jeden Network Load Balancer und Application Load Balancer, um sicherzustellen, dass mindestens eine fehlerfreie Amazon-Instance vorhanden ist. EC2
- ElbV2State: Prüft jeden Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie sich im richtigen Zustand befinden. `ACTIVE`
- ElbV2IpAddressType: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie dieselben IP-Adresstypen haben.
- ElbV2Scheme: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie dasselbe Schema haben.
- ElbV2Type: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie vom gleichen Typ sind.

- ElbV2S3LogsEnabled: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie denselben Wert für Amazon S3-Serverzugriffsprotokolle haben (AKTIVIERT oder DEAKTIVIERT).
- ElbV2DeletionProtection: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie den gleichen Wert für den Löschschutz haben (AKTIVIERT oder DEAKTIVIERT).
- ElbV2IdleTimeoutSeconds: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie für Sekunden im Leerlauf den gleichen Wert haben.
- ElbV2HttpDropInvalidHeaders: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie denselben Wert für HTTP Drop Invalid Header haben.
- ElbV2Http2Enabled: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie denselben Wert für (ENABLED oder DISABLED) haben. HTTP2
- ElbV2CrossZoneEnabled: Überprüft alle Network Load Balancer und Application Load Balancer, um sicherzustellen, dass sie den gleichen Wert für den zonenübergreifenden Load Balancing haben (AKTIVIERT oder DEAKTIVIERT).
- ElbV2ProvisionedCapacityLcuCount: Überprüft alle Network Load Balancer und Application Load Balancer mit einer bereitgestellten LCU von mehr als 10, um sicherzustellen, dass sie sich innerhalb von 20% der am höchsten bereitgestellten LCU in der Ressourcengruppe befinden.
- ElbV2ProvisionedCapacityEnabled: Prüft den Status der bereitgestellten Kapazität aller Network Load Balancers und Application Load Balancers, um sicherzustellen, dass sie nicht den Wert DISABLED oder PENDING haben.

Amazon-MSK-Cluster

- MskClusterClientSubnet: Prüft jeden MSK-Cluster, um sicherzustellen, dass er nur zwei oder nur drei Client-Subnetze hat.
- MskClusterInstanceType: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben EC2 Amazon-Instance-Typ haben.
- MskClusterSecurityGroups: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie dieselben Sicherheitsgruppen haben.
- MskClusterStorageInfo: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie dieselbe EBS-Speichervolumengröße haben. Wenn einer einen höheren Wert hat, werden die anderen als NICHT BEREIT markiert.
- MskClusterACMCertificate: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie über dieselbe Liste von Client-Autorisierungszertifikaten verfügen. ARNs

- MskClusterServerProperties: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Current Broker Software Info`
- MskClusterKafkaVersion: Prüft alle MSK-Cluster, um sicherzustellen, dass sie dieselbe Kafka-Version haben.
- MskClusterEncryptionInTransitInCluster: Prüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Encryption In Transit In Cluster`
- MskClusterEncryptionInClientBroker: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Encryption In Transit Client Broker`
- MskClusterEnhancedMonitoring: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Enhanced Monitoring`
- MskClusterOpenMonitoringInJmx: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Open Monitoring JMX Exporter`
- MskClusterOpenMonitoringInNode: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert haben für `Open Monitoring Not Exporter.`
- MskClusterLoggingInS3: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Is Logging in S3`
- MskClusterLoggingInFirehose: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Is Logging In Firehose`
- MskClusterLoggingInCloudWatch: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Is Logging Available In CloudWatch Logs`
- MskClusterNumberOfBrokerNodes: Überprüft alle MSK-Cluster, um sicherzustellen, dass sie denselben Wert für haben. `Number of Broker Nodes` Wenn einer einen höheren Wert hat, werden die anderen als NICHT BEREIT markiert.
- MskClusterState: Prüft jeden MSK-Cluster, um sicherzustellen, dass er sich im Status AKTIV befindet.
- MskClusterLimitsRule: Überprüft alle Lambda-Funktionen, um sicherzustellen, dass sie den von Service Quotas verwalteten Quotas (Grenzwerten) entsprechen.

Amazon Route 53-Zustandsprüfungen

- R53HealthCheckType: Prüft jeden Route 53 53-Zustandscheck, um sicherzustellen, dass er nicht vom Typ BERECHNET ist und dass alle Checks vom gleichen Typ sind.
- R53HealthCheckDisabled: Überprüft jede Route 53 53-Zustandsprüfung, um sicherzustellen, dass sie nicht den Status DEAKTIVIERT hat.

- R53HealthCheckStatus: Prüft jede Route 53 53-Zustandsprüfung, um sicherzustellen, dass sie den Status SUCCESS hat.
- R53HealthCheckRequestInterval: Überprüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass sie alle denselben Wert für `Request Interval` haben.
- R53HealthCheckFailureThreshold: Überprüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass sie alle denselben Wert haben für `Failure Threshold.`
- R53HealthCheckEnableSNI: Überprüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass sie alle denselben Wert haben für `Enable SNI.`
- R53HealthCheckSearchString: Überprüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass sie alle denselben Wert haben für `Search String.`
- R53HealthCheckRegions: Überprüft alle Zustandsprüfungen der Route 53, um sicherzustellen, dass sie alle dieselbe Liste von AWS Regionen haben.
- R53HealthCheckMeasureLatency: Überprüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass sie alle denselben Wert für `Measure Latency` haben.
- R53HealthCheckInsufficientDataHealthStatus: Überprüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass sie alle denselben Wert für `Insufficient Data Health Status` haben.
- R53HealthCheckInverted: Prüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass sie alle invertiert oder nicht invertiert sind.
- R53HealthCheckResourcePath: Überprüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass sie alle denselben Wert für `Resource Path` haben.
- R53HealthCheckCloudWatchAlarm: Überprüft alle Route 53 53-Zustandsprüfungen, um sicherzustellen, dass die damit verbundenen CloudWatch Alarme dieselben Einstellungen und Konfigurationen haben.

Amazon SNS-Abonnement

- SnsSubscriptionProtocol: Überprüft alle SNS-Abonnements, um sicherzustellen, dass sie dasselbe Protokoll verwenden.
- SnsSubscriptionSqsLambdaEndpoint: Überprüft alle SNS-Abonnements mit Lambda- oder SQS-Endpunkten, um sicherzustellen, dass sie unterschiedliche Endpunkte haben.
- SnsSubscriptionNonAwsEndpoint: Überprüft alle SNS-Abonnements, die einen Endpunkttyp haben, der kein AWS Service ist, z. B. E-Mail, um sicherzustellen, dass die Abonnements denselben Endpunkt haben.

- SnsSubscriptionPendingConfirmation: Überprüft alle SNS-Abonnements, um sicherzustellen, dass sie denselben Wert für „Ausstehende Bestätigungen“ haben.
- SnsSubscriptionDeliveryPolicy: Überprüft alle SNS-Abonnements, die HTTP/S verwenden, um sicherzustellen, dass sie denselben Wert für „Gültiger Lieferzeitraum“ haben.
- SnsSubscriptionRawMessageDelivery: Überprüft alle SNS-Abonnements, um sicherzustellen, dass sie denselben Wert für „Raw Message Delivery“ haben.
- SnsSubscriptionFilter: Überprüft alle SNS-Abonnements, um sicherzustellen, dass sie denselben Wert für „Filter Policy“ haben.
- SnsSubscriptionRedrivePolicy: Überprüft alle SNS-Abonnements, um sicherzustellen, dass sie denselben Wert für „Redrive Policy“ haben.
- SnsSubscriptionEndpointEnabled: Überprüft alle SNS-Abonnements, um sicherzustellen, dass sie denselben Wert für „Endpoint Enabled“ haben.
- SnsSubscriptionLambdaEndpointValid: Überprüft alle SNS-Abonnements mit Lambda-Endpunkten, um sicherzustellen, dass sie über gültige Lambda-Endpunkte verfügen.
- SnsSubscriptionSqsEndpointValidRule: Überprüft alle SNS-Abonnements, die SQS-Endpunkte verwenden, um sicherzustellen, dass sie über gültige SQS-Endpunkte verfügen.
- SnsSubscriptionQuotas: Überprüft alle SNS-Abonnements, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Limits) entsprechen.

Amazon SNS-Themen

- SnsTopicDisplayName: Überprüft alle SNS-Themen, um sicherzustellen, dass sie denselben Wert für haben. `Display Name`
- SnsTopicDeliveryPolicy: Überprüft alle SNS-Themen, die HTTPS-Abonnenten haben, um sicherzustellen, dass sie dieselben haben. `EffectiveDeliveryPolicy`
- SnsTopicSubscription: Überprüft alle SNS-Themen, um sicherzustellen, dass sie für jedes ihrer Protokolle die gleiche Anzahl von Abonnenten haben.
- SnsTopicAwsKmsKey: Prüft alle SNS-Themen, um sicherzustellen, dass alle Themen oder keines der Themen einen Schlüssel hat. AWS KMS
- SnsTopicQuotas: Überprüft alle SNS-Themen, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Limits) entsprechen.

Amazon SQS-Warteschlangen

- SqsQueueType: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie alle denselben Wert für haben. `Type`

- SqsQueueDelaySeconds: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie alle denselben Wert für haben. `Delay Seconds`
- SqsQueueMaximumMessageSize: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie alle denselben Wert für haben. `Maximum Message Size`
- SqsQueueMessageRetentionPeriod: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie alle denselben Wert für haben. `Message Retention Period`
- SqsQueueReceiveMessageWaitTimeSeconds: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie alle denselben Wert für haben. `Receive Message Wait Time Seconds`
- SqsQueueRedrivePolicyMaxReceiveCount: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie alle denselben Wert für haben. `Redrive Policy Max Receive Count`
- SqsQueueVisibilityTimeout: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie alle denselben Wert für haben. `Visibility Timeout`
- SqsQueueContentBasedDeduplication: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie alle denselben Wert für haben. `Content-Based Deduplication`
- SqsQueueQuotas: Überprüft alle SQS-Warteschlangen, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Limits) entsprechen.

Amazon VPCs

- VpcCidrBlock: Überprüft alle, VPCs um sicherzustellen, dass sie alle den gleichen Wert für die CIDR-Blocknetzwerkgröße haben.
- VpcCidrBlocksSameProtocolVersion: Überprüft alle Blöcke mit denselben CIDR-Blöcken VPCs , um sicherzustellen, dass sie denselben Wert für die Versionsnummer des Internet Stream Protocol haben.
- VpcCidrBlocksStateInAssociationSets: Überprüft alle CIDR-Blockzuordnungssätze für alle, VPCs um sicherzustellen, dass sie alle CIDR-Blöcke haben, die sich in einem bestimmten Status befinden. `ASSOCIATED`
- VpcIpv6CidrBlocksStateInAssociationSets: Überprüft alle CIDR-Blockzuordnungssätze für alle, VPCs um sicherzustellen, dass sie alle CIDR-Blöcke mit derselben Anzahl von Adressen haben.
- VpcCidrBlocksInAssociationSets: Überprüft alle CIDR-Blockzuordnungssätze für alle VPCs , um sicherzustellen, dass sie alle dieselbe Größe haben.
- VpcIpv6CidrBlocksInAssociationSets: Überprüft alle IPv6 CIDR-Blockzuordnungssätze für alle VPCs , um sicherzustellen, dass sie dieselbe Größe haben.

- VpcState: Prüft jede VPC, um sicherzustellen, dass sie sich in einem `AVAILABLE` bestimmten Zustand befindet.
- VpcInstanceTenancy: Prüft alle VPCs , um sicherzustellen, dass sie alle den gleichen Wert für haben. `Instance Tenancy`
- VpcIsDefault: Überprüft alle VPCs , um sicherzustellen, dass sie den gleichen Wert haben für `Is Default.`
- VpcSubnetState: Prüft jedes VPC-Subnetz, um sicherzustellen, dass es sich im Status AVAILABLE befindet.
- VpcSubnetAvailableIpAddressCount: Prüft jedes VPC-Subnetz, um sicherzustellen, dass die Anzahl der verfügbaren IP-Adressen größer als Null ist.
- VpcSubnetCount: Überprüft alle VPC-Subnetze, um sicherzustellen, dass sie dieselbe Anzahl von Subnetzen haben.
- VpcQuotas: Überprüft alle VPC-Subnetze, um sicherzustellen, dass sie den von Service Quotas verwalteten Kontingenten (Limits) entsprechen.

AWS VPN Verbindungen

- VpnConnectionsRouteCount: Überprüft alle VPN-Verbindungen, um sicherzustellen, dass sie mindestens eine Route und auch dieselbe Anzahl von Routen haben.
- VpnConnectionsEnableAcceleration: Überprüft alle VPN-Verbindungen, um sicherzustellen, dass sie denselben Wert für haben. `Enable Accelerations`
- VpnConnectionsStaticRoutesOnly: Überprüft alle VPN-Verbindungen, um sicherzustellen, dass sie denselben Wert haben für `Static Routes Only.`
- VpnConnectionsCategory: Überprüft alle VPN-Verbindungen, um sicherzustellen, dass sie eine Kategorie von haben. `VPN`
- VpnConnectionsCustomerConfiguration: Überprüft alle VPN-Verbindungen, um sicherzustellen, dass sie denselben Wert für haben. `Customer Gateway Configuration`
- VpnConnectionsCustomerGatewayId: Prüft jede VPN-Verbindung, um sicherzustellen, dass ein Kunden-Gateway angeschlossen ist.
- VpnConnectionsRoutesState: Überprüft alle VPN-Verbindungen, um sicherzustellen, dass sie sich in einem `AVAILABLE` einwandfreien Zustand befinden.
- VpnConnectionsVgwTelemetryStatus: Prüft jede VPN-Verbindung, um sicherzustellen, dass sie den VGW-Status von hat. `UP`
- VpnConnectionsVgwTelemetryIpAddress: Überprüft jede VPN-Verbindung, um sicherzustellen, dass sie für jede VGW-Telemetrie eine andere externe IP-Adresse hat.

- VpnConnectionsTunnelOptions: Überprüft alle VPN-Verbindungen, um sicherzustellen, dass sie dieselben Tunneloptionen haben.
- VpnConnectionsRoutesCidr: Prüft alle VPN-Verbindungen, um sicherzustellen, dass sie dieselben CIDR-Zielblöcke haben.
- VpnConnectionsInstanceType: Prüft alle VPN-Verbindungen, um sicherzustellen, dass sie dieselben haben. `Instance Type`

AWS VPN Gateways

- VpnGatewayState: Überprüft alle VPN-Gateways, um sicherzustellen, dass sie sich im Status VERFÜGBAR befinden.
- VpnGatewayAsn: Überprüft alle VPN-Gateways, um sicherzustellen, dass sie dieselbe ASN haben.
- VpnGatewayType: Überprüft alle VPN-Gateways, um sicherzustellen, dass sie denselben Typ haben.
- VpnGatewayAttachment: Überprüft alle VPN-Gateways, um sicherzustellen, dass sie dieselben Anhangskonfigurationen haben.

Bereitschaftsregeln auf der Konsole anzeigen

Sie können die Bereitschaftsregeln auf der einsehen AWS Management Console, die nach den einzelnen Ressourcentypen aufgelistet sind.

Um Bereitschaftsregeln auf der Konsole anzuzeigen

1. Öffnen Sie die ARC-Konsole unterhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Wählen Sie Readiness Check.
3. Wählen Sie unter Ressourcentyp den Ressourcentyp aus, für den Sie die Regeln anzeigen möchten.

Ressourcentypen und ARN-Formate in ARC

Wenn Sie einen Ressourcensatz in Amazon Application Recovery Controller (ARC) erstellen, geben Sie den Ressourcentyp an, der in den Satz aufgenommen werden soll, und die Amazon-Ressourcennamen (ARNs) für jede der einzuschließenden Ressourcen. ARC erwartet für jeden

Ressourcentyp ein bestimmtes ARN-Format. In diesem Abschnitt sind die von ARC unterstützten Ressourcentypen und die zugehörigen ARN-Formate für jeden einzelnen aufgeführt.

Das spezifische Format hängt von der Ressource ab. Wenn Sie einen ARN angeben, ersetzen Sie den *italicized* Text durch Ihre ressourcenspezifischen Informationen.

> **Note**
>
> Beachten Sie, dass das ARN-Format, das ARC für Ressourcen benötigt, sich von dem ARN-Format unterscheiden kann, das ein Dienst selbst für seine Ressourcen benötigt. Beispielsweise enthalten die ARN-Formate, die in den Abschnitten Ressourcentyp für jeden Dienst in der Service Authorization Reference beschrieben werden, möglicherweise nicht die AWS-Konto ID oder andere Informationen, die ARC benötigt, um Funktionen im ARC-Dienst zu unterstützen.

AWS::ApiGateway::Stage

Eine Stufe der Version 1 von Amazon API Gateway.

- ARN-Format: `arn:`*`partition`*`:apigateway:`*`region`*`:`*`account`*`:/restapis/`*`api-id`*`/stages/`*`stage-name`*

  Beispiel: `arn:aws:apigateway:us-east-1:111122223333:/restapis/123456789/stages/ExampleStage`

  Weitere Informationen finden Sie unter API Gateway Amazon Resource Name (ARN) - Referenz.

AWS::ApiGatewayV2::Stage

Eine Stufe der Version 2 von Amazon API Gateway.

- ARN-Format: `arn:`*`partition`*`:apigateway:`*`region`*`:`*`account`*`:/apis/`*`api-id`*`/stages/`*`stage-name`*

  Beispiel: `arn:aws:apigateway:us-east-1:111122223333:/apis/123456789/stages/ExampleStage`

  Weitere Informationen finden Sie unter API Gateway Amazon Resource Name (ARN) - Referenz.

AWS::CloudWatch::Alarm

Ein CloudWatch Amazon-Alarm.

- ARN-Format: `arn:partition:cloudwatch:region:account:alarm:alarm-name`

  Beispiel: `arn:aws:cloudwatch:us-west-2:111122223333:alarm:test-alarm-1`

  Weitere Informationen finden Sie unter Von Amazon definierte Ressourcentypen CloudWatch.

AWS::DynamoDB::Table

Eine Amazon DynamoDB-Tabelle.

- ARN-Format: `arn:partition:dynamodb:region:account:table/table-name`

  Beispiel: `arn:aws:dynamodb:us-west-2:111122223333:table/BigTable`

  Weitere Informationen finden Sie unter DynamoDB-Ressourcen und -Operationen.

AWS::EC2::CustomerGateway

Ein Kunden-Gateway-Gerät.

- ARN-Format: `arn:partition:ec2:region:account:customer-gateway/CustomerGatewayId`

  Beispiel: `arn:aws:ec2:us-west-2:111122223333:customer-gateway/vcg-123456789`

  Weitere Informationen finden Sie unter Von Amazon definierte Ressourcentypen EC2.

AWS::EC2::Volume

Ein Amazon EBS-Volume.

- ARN-Format: `arn:partition:ec2:region:account:volume/VolumeId`

  Beispiel: `arn:aws:ec2:us-west-2:111122223333:volume/volume-of-cylinder-is-pi`

  Weitere Informationen finden Sie unter API Gateway Amazon Resource Name (ARN) - Referenz.

AWS::ElasticLoadBalancing::LoadBalancer

Ein Classic Load Balancer.

- ARN-Format: `arn:partition:elasticloadbalancing:region:account:loadbalancer/LoadBalancerN`

  Beispiel: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/123456789abcbdeCLB`

  Weitere Informationen finden Sie unter Elastic Load Balancing Balancing-Ressourcen.

AWS::ElasticLoadBalancingV2::LoadBalancer

Ein Network Load Balancer oder ein Application Load Balancer.

- ARN-Format für Network Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Beispiel für Network Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdeNLB`
- ARN-Format für Application Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/app/LoadBalancerName`

  Beispiel für Application Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/app/sandbox-alb/123456789acbdeALB`

  Weitere Informationen finden Sie unter Elastic Load Balancing Balancing-Ressourcen.

AWS::Lambda::Function

Eine AWS Lambda Funktion.

- ARN-Format: `arn:partition:lambda:region:account:function:FunctionName`

  Beispiel: `arn:aws:lambda:us-west-2:111122223333:function:my-function`

  Weitere Informationen finden Sie unter Ressourcen und Bedingungen für Lambda-Aktionen.

AWS::MSK::Cluster

Ein Amazon-MSK-Cluster.

- ARN-Format: `arn:partition:kafka:region:account:cluster/ClusterName/UUID`

  Beispiel: `arn:aws:kafka:us-east-1:111122223333:cluster/demo-cluster-1/123456-1111-2222-3333`

Weitere Informationen finden Sie unter Von Amazon Managed Streaming for Apache Kafka definierte Ressourcentypen.

AWS::RDS::DBCluster

Ein Aurora-DB-Cluster.

- ARN-Format: `arn:partition:rds:region:account:cluster:DbClusterInstanceName`

  Beispiel: `arn:aws:rds:us-west-2:111122223333:cluster:database-1`

  Weitere Informationen finden Sie unter Arbeiten mit Amazon Resource Names (ARNs) in Amazon RDS.

AWS::Route53::HealthCheck

Ein Amazon Route 53-Gesundheitscheck.

- ARN-Format: `arn:partition:route53:::healthcheck/Id`

  Beispiel: `arn:aws:route53:::healthcheck/123456-1111-2222-3333`

AWS::SQS::Queue

Eine Amazon SQS SQS-Warteschlange.

- ARN-Format: `arn:partition:sqs:region:account:QueueName`

  Beispiel: `arn:aws:sqs:us-west-2:111122223333:StandardQueue`

  Weitere Informationen finden Sie unter Ressourcen und Abläufe für Amazon Simple Queue Service.

AWS::SNS::Topic

Amazon SNS-Thema.

- ARN-Format: `arn:partition:sns:region:account:TopicName`

  Beispiel: `arn:aws:sns:us-west-2:111122223333:TopicName`

  Weitere Informationen finden Sie unter ARN-Format für Amazon SNS SNS-Ressourcen.

AWS::SNS::Subscription

Ein Amazon SNS SNS-Abonnement.

- ARN-Format: `arn:partition:sns:region:account:TopicName:SubscriptionId`

  Beispiel: `arn:aws:sns:us-west-2:111122223333:TopicName:12345678901234567890`

AWS::EC2::VPC

Eine Virtual Private Cloud (VPC).

- ARN-Format: `arn:partition:ec2:region:account:vpc/VpcId`

  Beispiel: `arn:aws:ec2:us-west-2:111122223333:vpc/vpc-123456789`

  Weitere Informationen finden Sie unter VPC-Ressourcen.

AWS::EC2::VPNConnection

Eine VPN-Verbindung (Virtual Private Network).

- ARN-Format: `arn:partition:ec2:region:account:vpn-connection/VpnConnectionId`

  Beispiel: `arn:aws:ec2:us-west-2:111122223333:vpn-connection/vpn-123456789`

  Weitere Informationen finden Sie unter Von Amazon definierte Ressourcentypen EC2.

AWS::EC2::VPNGateway

Ein VPN-Gateway (Virtual Private Network).

- ARN-Format: `arn:partition:ec2:region:account:vpn-gateway/VpnGatewayId`

  Beispiel: `arn:aws:ec2:us-west-2:111122223333:vpn-gateway/vgw-123456789acbdefgh`

  Weitere Informationen finden Sie unter Von Amazon definierte Ressourcentypen EC2.

AWS::Route53RecoveryReadiness::DNSTargetResource

Eine DNS-Zielressource für Bereitschaftsprüfungen umfasst den DNS-Eintragstyp, den Domänennamen, den ARN für die gehostete Route 53-Zone und den Network Load Balancer ARN oder die Route 53-Datensatz-ID.

- ARN-Format für die gehostete Zone: `arn:partition:route53::account:hostedzone/Id`

Beispiel für eine gehostete Zone: `arn:aws:route53::111122223333:hostedzone/abcHostedZone`

HINWEIS: Sie müssen die Konto-ID in der gehosteten Zone angeben ARNs, wie hier angegeben. Die Konto-ID ist erforderlich, damit ARC die Ressource abfragen kann. Das Format unterscheidet sich bewusst von dem ARN-Format, das Amazon Route 53 benötigt und das in den Route 53-Service Resource types in der Service Authorization Reference beschrieben ist.

- ARN-Format für Network Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Beispiel für Network Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdefgh`

  Weitere Informationen finden Sie unter Elastic Load Balancing Balancing-Ressourcen.

Protokollierung und Überwachung für die Bereitschaftsprüfung im Amazon Application Recovery Controller (ARC)

Sie können Amazon CloudWatch AWS CloudTrail, und Amazon EventBridge zur Überwachung der Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC) verwenden, um Muster zu analysieren und Probleme zu beheben.

> **Note**
>
> Sie müssen CloudWatch Metriken und Protokolle für ARC in der Region USA West (Oregon) sowohl in der Konsole als auch bei der Verwendung von anzeigen AWS CLI. Wenn Sie den verwenden AWS CLI, geben Sie die Region USA West (Oregon) für Ihren Befehl an, indem Sie den folgenden Parameter angeben:`--region us-west-2`.

Themen

- Amazon CloudWatch mit Bereitschaftsprüfung in ARC verwenden
- Protokollierung von API-Aufrufen zur Bereitschaftsprüfung mit AWS CloudTrail
- Bereitschaftsprüfung in ARC mit Amazon verwenden EventBridge

Amazon CloudWatch mit Bereitschaftsprüfung in ARC verwenden

Amazon Application Recovery Controller (ARC) veröffentlicht Datenpunkte CloudWatch für Ihre Bereitschaftsprüfungen an Amazon. CloudWatch ermöglicht es Ihnen, Statistiken über diese Datenpunkte in Form eines geordneten Satzes von Zeitreihendaten, sogenannten Metriken, abzurufen. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Sie können beispielsweise den Verkehr in einer AWS Region über einen bestimmten Zeitraum überwachen. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können beispielsweise einen CloudWatch Alarm erstellen, um eine bestimmte Metrik zu überwachen und eine Aktion einzuleiten (z. B. das Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb des für Sie akzeptablen Bereichs liegt.

Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Themen

- ARC-Metriken
- Statistiken für ARC-Metriken
- CloudWatch Metriken in ARC anzeigen

ARC-Metriken

Der `AWS/Route53RecoveryReadiness`-Namespace enthält die folgenden Metriken.

Metrik	Beschreibung
`ReadinessChecks`	Stellt die Anzahl der von ARC verarbeiteten Bereitschaftsprüfungen dar. Die Metrik kann anhand ihrer Status dimensioniert werden, die unten aufgeführt sind. Einheit:`Count`. Berichtkriterien: Ein Wert ungleich Null. Statistik: Die einzig nützliche Statistik ist`Sum`.

Metrik	Beschreibung
	Dimensionen • READY • NOT_READY • NOT_AUTHORIZED • UNKNOWN
Resources	Stellt die Anzahl der von ARC verarbeiteten Ressourcen dar, die anhand ihrer in der API definierten Ressourcen-ID dimensioniert werden kann. Einheit:Count. Berichtkriterien: Ein Wert ungleich Null. Statistik: Die einzig nützliche Statistik istSum. Dimensionen • ResourceSetType : Dies sind die Ressourcentypen, gefiltert nach der Anzahl der Ressourcen pro gegebenem Typ, die von ARC bewertet wurden Zum Beispiel: AWS::CloudWatch::Alarm

Statistiken für ARC-Metriken

CloudWatch bietet Statistiken, die auf den von ARC veröffentlichten metrischen Datenpunkten basieren. Statistiken sind Aggregationen metrischer Daten über einen bestimmten Zeitraum. Wenn Sie Statistiken anfordern, wird der zurückgegebene Datenstrom durch den Metriknamen und die Dimension identifiziert. Eine Dimension ist ein Name-Wert-Paar, durch das eine Metrik eindeutig identifiziert wird.

Im Folgenden finden Sie Beispiele für Kombinationen aus Metrik und Dimension, die für Sie nützlich sein könnten:

- Sehen Sie sich die Anzahl der Bereitschaftsprüfungen an, die von ARC auf ihre Bereitschaft hin bewertet wurden.
- Zeigt die Gesamtzahl der Ressourcen für einen bestimmten Ressourcentyp an, die von ARC bewertet wurden.

CloudWatch Metriken in ARC anzeigen

Sie können die CloudWatch Metriken für ARC in der CloudWatch Konsole oder im anzeigen AWS CLI. In der Konsole werden die Metriken als Monitoring-Graphen angezeigt.

Sie müssen die CloudWatch Metriken für ARC in der Region USA West (Oregon) sowohl in der Konsole als auch bei der Verwendung von anzeigen AWS CLI. Wenn Sie den verwenden AWS CLI, geben Sie die Region USA West (Oregon) für Ihren Befehl an, indem Sie den folgenden Parameter angeben:`--region us-west-2`.

Um Metriken mit der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den Route53-Namespace RecoveryReadiness aus.
4. (Optional) Um eine Metrik für alle Dimensionen anzuzeigen, geben Sie den Namen in das Suchfeld ein.

Um Metriken mit dem anzuzeigen AWS CLI

Verwenden Sie den folgenden list-metrics-Befehl, um die verfügbaren Metriken aufzuführen:

```
aws cloudwatch list-metrics --namespace AWS/Route53RecoveryReadiness --region us-west-2
```

Um die Statistiken für eine Metrik abzurufen, verwenden Sie AWS CLI

Verwenden Sie den folgenden get-metric-statisticsBefehl, um Statistiken für eine angegebene Metrik und Dimension abzurufen. Beachten Sie, dass jede eindeutige Kombination von Dimensionen als separate Metrik CloudWatch behandelt wird. Sie können keine Statistiken abrufen, die Kombinationen von Dimensionen verwenden, die nicht ausdrücklich veröffentlicht wurden. Sie müssen die gleichen Dimensionen angeben, die bei der Erstellung der Metriken verwendet wurden.

Das folgende Beispiel listet die Gesamtzahl der pro Minute ausgewerteten Bereitschaftsprüfungen für ein Konto in ARC auf.

```
aws cloudwatch get-metric-statistics --namespace AWS/Route53RecoveryReadiness \
--metric-name ReadinessChecks \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=State,Value=READY \
--start-time 2021-07-03T01:00:00Z --end-time 2021-07-03T01:20:00Z
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe des Befehls:

```
{
    "Label": "ReadinessChecks",
    "Datapoints": [
        {
            "Timestamp": "2021-07-08T18:00:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:04:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:01:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:02:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:03:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        }
    ]
}
```

Protokollierung von API-Aufrufen zur Bereitschaftsprüfung mit AWS CloudTrail

ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ARC ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für ARC als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der ARC-Konsole und Codeaufrufen für die ARC-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für ARC. 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 CloudTrail, die an ARC gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

ARC-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in ARC eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für ARC, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail

- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle ARC-Aktionen werden im Recovery Readiness API-Referenzhandbuch für Amazon Application Recovery Controller, im Recovery Control Configuration API-Referenzhandbuch für Amazon Application Recovery Controller und im Routing Control API-Referenzhandbuch für Amazon Application Recovery Controller protokolliert und dokumentiert. CloudTrail Beispielsweise generieren Aufrufe von `UpdateRoutingControlState` und `CreateRecoveryGroup` Aktionen Einträge in den CloudTrail Protokolldateien. `CreateCluster`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

ARC-Ereignisse im Ereignisverlauf anzeigen

CloudTrail ermöglicht es Ihnen, aktuelle Ereignisse im Event-Verlauf einzusehen. Um Ereignisse für ARC-API-Anfragen anzuzeigen, müssen Sie in der Regionsauswahl oben in der Konsole die Option USA West (Oregon) auswählen. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Grundlegendes zu ARC-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateRecoveryGroup` Aktion für die Bereitschaftsprüfung demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA33L3W36EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/admin",
                "accountId": "111122223333",
                "userName": "EXAMPLENAME"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-07-06T17:38:05Z"
            }
        }
    },
    "eventTime": "2021-07-06T18:08:03Z",
    "eventSource": "route53-recovery-readiness.amazonaws.com",
    "eventName": "CreateRecoveryGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
    "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
    "requestParameters": {
        "recoveryGroupName": "MyRecoveryGroup"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-errortype,x-amzn-requestid,x-amzn-
errormessage,x-amzn-trace-id,x-amzn-requestid,x-amz-apigw-id,date",
        "cells": [],
        "recoveryGroupName": "MyRecoveryGroup",
        "recoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/MyRecoveryGroup",
        "tags": "***"
    },
    "requestID": "fd42dcf7-6446-41e9-b408-d096example",
```

```
    "eventID": "4b5c42df-1174-46c8-be99-d67aexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

Bereitschaftsprüfung in ARC mit Amazon verwenden EventBridge

Mithilfe von Amazon können Sie ereignisgesteuerte Regeln einrichten EventBridge, die Ihre Ressourcen zur Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC) überwachen und dann Zielaktionen einleiten, die andere AWS Services nutzen. Sie können beispielsweise eine Regel für das Versenden von E-Mail-Benachrichtigungen festlegen, indem Sie ein Amazon SNS SNS-Thema signalisieren, wenn sich der Status einer Bereitschaftsprüfung von READY auf NOT READY ändert.

> **Note**
>
> ARC veröffentlicht nur EventBridge Veranstaltungen für die Bereitschaftsprüfung in der Region USA West (Oregon) (us-west-2) AWS . Erstellen Sie EventBridge Regeln in der Region USA West (Oregon), um EventBridge Ereignisse für die Eignungsprüfung zu erhalten.

Sie können in Amazon Regeln erstellen EventBridge , um auf das folgende ARC-Bereitschaftsprüfungsereignis zu reagieren:

- Bereitschaft prüfen, ob bereit ist. Das Ereignis gibt an, ob sich der Status der Bereitschaftsprüfung ändert, z. B. von BEREIT zu NICHT BEREIT.

Um bestimmte ARC-Ereignisse zu erfassen, an denen Sie interessiert sind, definieren Sie ereignisspezifische Muster, anhand derer die Ereignisse erkannt EventBridge werden können. Ereignismuster haben dieselbe Struktur wie die Ereignisse, denen sie entsprechen. Das Muster zitiert die Felder, die Sie abgleichen möchten, und liefert die Werte, nach denen Sie suchen.

Ereignisse werden auf bestmögliche Weise ausgegeben. Sie werden unter normalen Betriebsbedingungen nahezu EventBridge in Echtzeit von ARC an übermittelt. Es können jedoch Situationen auftreten, die die Durchführung eines Ereignisses verzögern oder verhindern können.

Informationen darüber, wie EventBridge Regeln mit Ereignismustern funktionieren, finden Sie unter Ereignisse und Ereignismuster in EventBridge.

Überwachen Sie eine Ressource zur Eignungsprüfung mit EventBridge

Mit können Sie Regeln erstellen EventBridge, die Aktionen definieren, die ergriffen werden sollen, wenn ARC Ereignisse für Ressourcen zur Bereitschaftsprüfung ausgibt.

Um ein Ereignismuster einzugeben oder zu kopieren und in die EventBridge Konsole einzufügen, wählen Sie in der Konsole die Option Eigene Eingabe aus. Um Ihnen bei der Bestimmung von Ereignismustern zu helfen, die für Sie nützlich sein könnten, enthält dieses Thema Beispiele für Bereitschaftsereignisse.

So erstellen Sie eine Regel für ein Ressourcenereignis

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. AWS-Region Um die Regel zu erstellen, wählen Sie US West (Oregon). Dies ist die erforderliche Region für Bereitschaftsereignisse.
3. Wählen Sie Create rule (Regel erstellen) aus.
4. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.
5. Behalten Sie für Event Bus den Standardwert default bei.
6. Wählen Sie Weiter.
7. Behalten Sie für den Schritt Ereignismuster erstellen für Ereignisquelle den Standardwert AWS Ereignisse bei.
8. Wählen Sie unter Beispielereignis die Option Eigenes Ereignis eingeben aus.
9. Geben Sie für Beispielereignisse ein Ereignismuster ein oder kopieren Sie es und fügen Sie es ein. Beispiele finden Sie im nächsten Abschnitt.

Beispiele für Muster von Bereitschaftsereignissen

Ereignismuster haben dieselbe Struktur wie die Ereignisse, denen sie entsprechen. Das Muster zitiert die Felder, die Sie abgleichen möchten, und liefert die Werte, nach denen Sie suchen.

Sie können Ereignismuster aus diesem Abschnitt kopieren und einfügen, um Regeln EventBridge zu erstellen, mit denen Sie ARC-Aktionen und -Ressourcen überwachen können.

Die folgenden Ereignismuster enthalten Beispiele, die Sie EventBridge für die Funktion zur Bereitschaftsprüfung in ARC verwenden können.

- Wählen Sie alle Ereignisse aus der ARC-Bereitschaftsprüfung aus.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ]
}
```

- Wählen Sie nur Ereignisse aus, die sich auf Zellen beziehen.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ]
}
```

- Wählen Sie nur Ereignisse aus, die sich auf eine bestimmte aufgerufene Zelle beziehen *`MyExampleCell`*.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ],
    "resources": [
        "arn:aws:route53-recovery-readiness::111122223333:cell/MyExampleCell"
    ]
}
```

- Wählen Sie nur Ereignisse aus, wenn sich der Status einer Wiederherstellungsgruppe, Zelle oder Bereitschaftsprüfung ändert *`NOT READY`*.

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail-type":{
```

```
      "new-state":{
         "readiness-status":[
            "NOT_READY"
         ]
      }
   }
}
```

- Wählen Sie nur Ereignisse aus, wenn aus einer Wiederherstellungsgruppe, Zelle oder Bereitschaftsprüfung etwas anderes wird *READY*

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail":{
      "new-state":{
         "readiness-status":[
            {
               "anything-but":"READY"
            }
         ]
      }
   }
}
```

Im Folgenden finden Sie ein Beispiel für ein ARC-Ereignis für eine Änderung des Bereitschaftsstatus einer Wiederherstellungsgruppe:

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller recovery group readiness
 status change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:recovery-group/BillingApp"
    ],
    "detail": {
```

```
        "recovery-group-name": "BillingApp",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Im Folgenden finden Sie ein Beispiel für ein ARC-Ereignis für eine Änderung des Status der Zellbereitschaft:

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller cell readiness status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:cell/PDXCell"
    ],
    "detail": {
        "cell-name": "PDXCell",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Im Folgenden finden Sie ein Beispiel für ein ARC-Ereignis für eine Änderung des Status der Bereitschaftsprüfung:

```
{
    "version": "0",
    "account":"111122223333",
```

```
    "detail-type":"Route 53 Application Recovery Controller readiness check status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:readiness-check/
UserTableReadinessCheck"
    ],
    "detail": {
    "readiness-check-name": "UserTableReadinessCheck",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Geben Sie eine CloudWatch Protokollgruppe an, die als Ziel verwendet werden soll

Wenn Sie eine EventBridge Regel erstellen, müssen Sie das Ziel angeben, an das Ereignisse gesendet werden, die der Regel entsprechen. Eine Liste der verfügbaren Ziele für EventBridge finden Sie unter In der EventBridge Konsole verfügbare Ziele. Eines der Ziele, die Sie einer EventBridge Regel hinzufügen können, ist eine CloudWatch Amazon-Protokollgruppe. In diesem Abschnitt werden die Anforderungen für das Hinzufügen von CloudWatch Protokollgruppen als Ziele beschrieben und ein Verfahren zum Hinzufügen einer Protokollgruppe beim Erstellen einer Regel beschrieben.

Um eine CloudWatch Protokollgruppe als Ziel hinzuzufügen, können Sie einen der folgenden Schritte ausführen:

- Erstellen Sie eine neue Protokollgruppe
- Wählen Sie eine bestehende Protokollgruppe

Wenn Sie beim Erstellen einer Regel mithilfe der Konsole eine neue Protokollgruppe angeben, EventBridge wird die Protokollgruppe automatisch für Sie erstellt. Stellen Sie sicher, dass die Protokollgruppe, die Sie als Ziel für die EventBridge Regel verwenden, mit beginnt`/aws/events`. Wenn Sie eine bestehende Protokollgruppe auswählen möchten, beachten Sie, dass nur Protokollgruppen, die mit beginnen, als Optionen im Dropdownmenü `/aws/events` angezeigt

werden. Weitere Informationen finden Sie unter Neue Protokollgruppe erstellen im CloudWatch Amazon-Benutzerhandbuch.

Wenn Sie eine CloudWatch Protokollgruppe erstellen oder verwenden, um sie mithilfe von CloudWatch Vorgängen außerhalb der Konsole als Ziel zu verwenden, stellen Sie sicher, dass Sie die Berechtigungen korrekt festlegen. Wenn Sie die Konsole verwenden, um einer EventBridge Regel eine Protokollgruppe hinzuzufügen, wird die ressourcenbasierte Richtlinie für die Protokollgruppe automatisch aktualisiert. Wenn Sie jedoch das AWS Command Line Interface oder ein AWS SDK verwenden, um eine Protokollgruppe anzugeben, müssen Sie die ressourcenbasierte Richtlinie für die Protokollgruppe aktualisieren. Die folgende Beispielrichtlinie veranschaulicht die Berechtigungen, die Sie in einer ressourcenbasierten Richtlinie für die Protokollgruppe definieren müssen:

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

Sie können eine ressourcenbasierte Richtlinie für eine Protokollgruppe nicht mithilfe der Konsole konfigurieren. Verwenden Sie den API-Vorgang, um einer ressourcenbasierten Richtlinie die erforderlichen Berechtigungen hinzuzufügen. CloudWatch PutResourcePolicy Anschließend können Sie mit dem describe-resource-policiesCLI-Befehl überprüfen, ob Ihre Richtlinie korrekt angewendet wurde.

Um eine Regel für ein Ressourcenereignis zu erstellen und ein Ziel für die CloudWatch Protokollgruppe anzugeben

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie AWS-Region die aus, in der Sie die Regel erstellen möchten.
3. Wählen Sie Regel erstellen und geben Sie dann alle Informationen zu dieser Regel ein, z. B. das Ereignismuster oder Details zum Zeitplan.

   Weitere Informationen zum Erstellen von EventBridge Bereitschaftsregeln finden Sie unter Überwachen einer Ressource zur Eignungsprüfung mit EventBridge.
4. Wählen Sie auf der Seite „Ziel auswählen CloudWatch“ Ihr Ziel aus.
5. Wählen Sie eine CloudWatch Protokollgruppe aus dem Drop-down-Menü aus.

Identity and Access Management für die Prüfung der Eignung

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 ARC-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Inhalt

- So funktioniert Readiness Check SERVICElong In mit IAM
- Beispiele für identitätsbasierte Richtlinien für die Eignungsprüfung in Amazon Application Recovery Controller (ARC)
- Verwenden einer serviceverknüpften Rolle für die Bereitschaftsprüfung in ARC
- AWS verwaltete Richtlinien für die Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC)

So funktioniert Readiness Check SERVICElong In mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf ARC verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit ARC verfügbar sind.

Bevor Sie IAM verwenden, um den Zugriff auf die Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC) zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Bereitschaftsprüfung verfügbar sind.

IAM-Funktionen, die Sie mit der Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC) verwenden können

IAM-Feature	Unterstützung bei der Prüfung der Bereitschaft
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für die Prüfung der Eignung

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 ARC-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien in Amazon Application Recovery Controller (ARC)

Ressourcenbasierte Richtlinien im Rahmen der Eignungsprüfung

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.

Politische Maßnahmen für die Eignungsprüfung

Unterstützt Richtlinienaktionen: Ja

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

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 keinen passenden API-Vorgang 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 ARC-Aktionen für die Bereitschaftsprüfung finden Sie unter Von Amazon Route 53 Recovery Readiness definierte Aktionen in der Service Authorization Reference.

Bei den Richtlinienaktionen in ARC für die Bereitschaftsprüfung werden vor der Aktion die folgenden Präfixe verwendet:

```
route53-recovery-readiness
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata: Zum Beispiel das Folgende:

```
"Action": [
      "route53-recovery-readiness:action1",
      "route53-recovery-readiness:action2"
         ]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "route53-recovery-readiness:Describe*"
```

Beispiele für identitätsbasierte ARC-Richtlinien für die Eignungsprüfung finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Eignungsprüfung in Amazon Application Recovery Controller (ARC)

Richtlinienressourcen für die Prüfung der Eignung

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 ARC-Aktionen für Zonal Shift finden Sie unter Von Amazon Route 53 Recovery Readiness definierte Aktionen.

Beispiele für identitätsbasierte ARC-Richtlinien zur Bereitschaftsprüfung finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Eignungsprüfung in Amazon Application Recovery Controller (ARC)

Zustandsschlüssel für Richtlinien für die Prüfung der Bereitschaft

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 ARC-Aktionen für die Bereitschaftsprüfung finden Sie unter Bedingungsschlüssel für Amazon Route 53 Recovery Readiness

Informationen zu den Aktionen und Ressourcen, die Sie mit einem Bedingungsschlüssel mit Bereitschaftsprüfung verwenden können, finden Sie unter Von Amazon Route 53 Recovery Readiness definierte Aktionen

Beispiele für identitätsbasierte ARC-Richtlinien für die Eignungsprüfung finden Sie unter. Beispiele für identitätsbasierte Richtlinien für die Eignungsprüfung in Amazon Application Recovery Controller (ARC)

Zugriffskontrolllisten (ACLs) werden derzeit geprüft

Unterstützt ACLs: Nein

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

Attributbasierte Zugriffskontrolle (ABAC) mit Bereitschaftsprüfung

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt 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 Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

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

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Recovery Readiness (Bereitschaftsprüfung) unterstützt ABAC.

Verwendung temporärer Anmeldeinformationen mit Bereitschaftsprüfung

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 von einer Benutzerrolle zu einer IAM-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.

Dienstübergreifende Prinzipalberechtigungen für die Prüfung der Eignung

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie eine IAM-Entität (Benutzer oder Rolle) verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Richtlinien erteilen einem Prinzipal-Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen.

Informationen darüber, ob eine Aktion bei der Bereitschaftsprüfung zusätzliche abhängige Aktionen in einer Richtlinie erfordert, finden Sie unter Amazon Route 53 Recovery Readiness

Servicerollen für die Bereitschaftsprüfung

Unterstützt Servicerollen: Nein

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.

Dienstbezogene Rollen für die Prüfung der Eignung

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte 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. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen ARC-Rollen finden Sie unter. Verwenden einer serviceverknüpften Rolle für die Bereitschaftsprüfung in ARC

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für die Eignungsprüfung in Amazon Application Recovery Controller (ARC)

Standardmäßig sind Benutzer und Rollen nicht berechtigt, ARC-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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von ARC definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und

Bedingungsschlüssel für Amazon Application Recovery Controller (ARC) in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Beispiel: Konsolenzugriff mit Bereitschaftsprüfung
- Beispiele: API-Aktionen zur Bereitschaftsprüfung für die Bereitschaftsprüfung

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand ARC-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 Richtlinienvalidierung mit 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 Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Beispiel: Konsolenzugriff mit Bereitschaftsprüfung

Um auf die Amazon Application Recovery Controller (ARC) -Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den ARC-Ressourcen in Ihrem aufzulisten und anzuzeigen 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 API 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 Konsole für die Bereitschaftsprüfung weiterhin verwenden können, wenn Sie nur den Zugriff auf bestimmte API-Operationen zulassen, fügen Sie den Entitäten außerdem eine `ReadOnly` AWS verwaltete Richtlinie für die Bereitschaftsprüfung hinzu. Weitere Informationen finden Sie auf der Seite mit verwalteten Richtlinien zur Bereitschaftsprüfung zur Eignungsprüfung oder unter Hinzufügen von Benutzerberechtigungen im IAM-Benutzerhandbuch.

Um einige Aufgaben ausführen zu können, müssen Benutzer über die Berechtigung verfügen, die mit dem Dienst verknüpfte Rolle zu erstellen, die mit der Bereitschaftsprüfung in ARC verknüpft ist. Weitere Informationen hierzu finden Sie unter Verwenden einer serviceverknüpften Rolle für die Bereitschaftsprüfung in ARC.

Um Benutzern über die Konsole vollen Zugriff auf die Funktionen zur Eignungsprüfung zu gewähren, fügen Sie dem Benutzer eine Richtlinie wie die folgende hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-readiness:CreateCell",
                   "route53-recovery-readiness:CreateCrossAccountAuthorization",
                   "route53-recovery-readiness:CreateReadinessCheck",
                   "route53-recovery-readiness:CreateRecoveryGroup",
                   "route53-recovery-readiness:CreateResourceSet",
                   "route53-recovery-readiness:DeleteCell",
                   "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                   "route53-recovery-readiness:DeleteReadinessCheck",
                   "route53-recovery-readiness:DeleteRecoveryGroup",
                   "route53-recovery-readiness:DeleteResourceSet",
                   "route53-recovery-readiness:GetArchitectureRecommendations",
                   "route53-recovery-readiness:GetCell",
                   "route53-recovery-readiness:GetCellReadinessSummary",
                   "route53-recovery-readiness:GetReadinessCheck",
                   "route53-recovery-readiness:GetReadinessCheckResourceStatus",
                   "route53-recovery-readiness:GetReadinessCheckStatus",
                   "route53-recovery-readiness:GetRecoveryGroup",
                   "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                   "route53-recovery-readiness:GetResourceSet",
                   "route53-recovery-readiness:ListCells",
                   "route53-recovery-readiness:ListCrossAccountAuthorizations",
                   "route53-recovery-readiness:ListReadinessChecks",
                   "route53-recovery-readiness:ListRecoveryGroups",
                   "route53-recovery-readiness:ListResourceSets",
                   "route53-recovery-readiness:ListRules",
                   "route53-recovery-readiness:UpdateCell",
                   "route53-recovery-readiness:UpdateReadinessCheck",
                   "route53-recovery-readiness:UpdateRecoveryGroup",
                   "route53-recovery-readiness:UpdateResourceSet"
```

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

Beispiele: API-Aktionen zur Bereitschaftsprüfung für die Bereitschaftsprüfung

Um sicherzustellen, dass ein Benutzer ARC-API-Aktionen verwenden kann, um mit der ARC-Bereitschaftsprüfungsebene zu arbeiten — z. B. um Wiederherstellungsgruppen, Ressourcensätze und Bereitschaftsprüfungen zu erstellen — fügen Sie eine Richtlinie hinzu, die den API-Vorgängen entspricht, mit denen der Benutzer arbeiten muss, wie unten beschrieben.

Um einige Aufgaben ausführen zu können, müssen Benutzer über die Berechtigung verfügen, die mit dem Dienst verknüpfte Rolle zu erstellen, die mit der Bereitschaftsprüfung in ARC verknüpft ist. Weitere Informationen hierzu finden Sie unter Verwenden einer serviceverknüpften Rolle für die Bereitschaftsprüfung in ARC.

Um mit API-Operationen für die Prüfung der Eignung zu arbeiten, fügen Sie dem Benutzer eine Richtlinie wie die folgende hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-readiness:CreateCell",
                   "route53-recovery-readiness:CreateCrossAccountAuthorization",
                   "route53-recovery-readiness:CreateReadinessCheck",
                   "route53-recovery-readiness:CreateRecoveryGroup",
                   "route53-recovery-readiness:CreateResourceSet",
                   "route53-recovery-readiness:DeleteCell",
                   "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                   "route53-recovery-readiness:DeleteReadinessCheck",
                   "route53-recovery-readiness:DeleteRecoveryGroup",
                   "route53-recovery-readiness:DeleteResourceSet",
                   "route53-recovery-readiness:GetArchitectureRecommendations",
                   "route53-recovery-readiness:GetCell",
                   "route53-recovery-readiness:GetCellReadinessSummary",
                   "route53-recovery-readiness:GetReadinessCheck",
                   "route53-recovery-readiness:GetReadinessCheckResourceStatus",
```

```
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetRecoveryGroup",
                "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListCells",
                "route53-recovery-readiness:ListCrossAccountAuthorizations",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53-recovery-readiness:ListRecoveryGroups",
                "route53-recovery-readiness:ListResourceSets",
                "route53-recovery-readiness:ListRules",
                "route53-recovery-readiness:ListTagsForResources",
                "route53-recovery-readiness:UpdateCell",
                "route53-recovery-readiness:UpdateReadinessCheck",
                "route53-recovery-readiness:UpdateRecoveryGroup",
                "route53-recovery-readiness:UpdateResourceSet",
                "route53-recovery-readiness:TagResource",
                "route53-recovery-readiness:UntagResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Verwenden einer serviceverknüpften Rolle für die Bereitschaftsprüfung in ARC

Amazon Application Recovery Controller verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit einem Service verknüpft ist — in diesem Fall ARC. Servicebezogene Rollen sind von ARC vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um in Ihrem Namen andere AWS Dienste für bestimmte Zwecke aufzurufen.

Servicebezogene Rollen erleichtern die Einrichtung von ARC, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. ARC definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur ARC seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen juristischen Stelle von IAM zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre ARC-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entziehen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Dienstverknüpfte Rolle nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

ARC hat die folgenden dienstbezogenen Rollen, die in diesem Kapitel beschrieben werden:

- ARC verwendet die dienstgebundene Rolle Route53, RecoveryReadinessServiceRolePolicy um auf Ressourcen und Konfigurationen zuzugreifen und die Bereitschaft zu überprüfen.
- ARC verwendet die servicebezogene Rolle, die nach Autoshift-Übungsläufen benannt ist, um vom Kunden bereitgestellte CloudWatch Amazon-Alarme und AWS Health Dashboard Kundenereignisse zu überwachen und Übungsläufe zu starten.

Dienstbezogene Rollenberechtigungen für Route53 RecoveryReadinessServiceRolePolicy

ARC verwendet eine serviceverknüpfte Rolle namens Route53, RecoveryReadinessServiceRolePolicy um auf Ressourcen und Konfigurationen zuzugreifen und die Bereitschaft zu überprüfen. In diesem Abschnitt werden die Berechtigungen für die serviceverknüpfte Rolle sowie Informationen zum Erstellen, Bearbeiten und Löschen der Rolle beschrieben.

Berechtigungen für dienstverknüpfte Rollen für Route53 RecoveryReadinessServiceRolePolicy

Diese dienstverknüpfte Rolle verwendet die verwaltete Richtlinie. `Route53RecoveryReadinessServiceRolePolicy`

Die RecoveryReadinessServiceRolePolicy dienstverknüpfte Route53-Rolle vertraut darauf, dass der folgende Dienst die Rolle übernimmt:

- `route53-recovery-readiness.amazonaws.com`

Die Berechtigungen für diese Richtlinie finden Sie unter Route53 RecoveryReadinessServiceRolePolicy in der Referenz für verwaltete Richtlinien.AWS

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Die serviceverknüpfte Route53-Rolle RecoveryReadinessServiceRolePolicy für ARC erstellen

Sie müssen die serviceverknüpfte RecoveryReadinessServiceRolePolicyRoute53-Rolle nicht manuell erstellen. Wenn Sie die erste Bereitschaftsprüfung oder die kontoübergreifende Autorisierung in der AWS Management Console, der oder der AWS API erstellen AWS CLI, erstellt ARC die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie die erste Eignungsprüfung oder die kontoübergreifende Autorisierung erstellen, erstellt ARC erneut die dienstbezogene Rolle für Sie.

Bearbeitung der RecoveryReadinessServiceRolePolicy serviceverknüpften Route53-Rolle für ARC

In ARC können Sie die serviceverknüpfte RecoveryReadinessServiceRolePolicyRoute53-Rolle nicht bearbeiten. Nachdem Sie die dienstverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da andere Entitäten möglicherweise auf die Rolle verweisen. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der RecoveryReadinessServiceRolePolicy dienstverknüpften Route53-Rolle für ARC

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Nachdem Sie Ihre Eignungsüberprüfungen und Ihre kontoübergreifenden Autorisierungen entfernt haben, können Sie die dienstverknüpfte Route53-Rolle löschen. RecoveryReadinessServiceRolePolicy Weitere Informationen zu Bereitschaftsprüfungen finden Sie unter. Bereitschaftsprüfung in ARC Weitere Informationen zu kontoübergreifenden Autorisierungen finden Sie unter. Kontoübergreifende Autorisierungen in ARC erstellen

> **Note**
>
> Wenn der ARC-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen der Servicerolle möglicherweise fehl. Warten Sie in diesem Fall einige Minuten und versuchen Sie erneut, die Rolle zu löschen.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die dienstverknüpfte RecoveryReadinessServiceRolePolicy Route53-Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Aktualisierungen der dienstverknüpften ARC-Rolle für die Prüfung der Eignung

Aktualisierungen der AWS verwalteten Richtlinien für die mit dem ARC-Dienst verknüpften Rollen finden Sie in der Tabelle mit Aktualisierungen AWS verwalteter Richtlinien für ARC. Sie können auch automatische RSS-Benachrichtigungen auf der Seite mit dem Verlauf der ARC-Dokumente abonnieren.

AWS verwaltete Richtlinien für die Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC)

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, 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 für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete 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.

AWS verwaltete Richtlinie: Route53 RecoveryReadinessServiceRolePolicy

Sie können `Route53RecoveryReadinessServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer servicebezogenen Rolle verknüpft, die es Amazon Application Recovery Controller (ARC) ermöglicht, auf AWS Dienste und Ressourcen zuzugreifen, die von ARC verwendet oder verwaltet werden. Weitere Informationen finden Sie unter Verwenden einer serviceverknüpften Rolle für die Bereitschaftsprüfung in ARC.

AWS verwaltete Richtlinie: 53 AmazonRoute RecoveryReadinessFullAccess

Sie können `AmazonRoute53RecoveryReadinessFullAccess` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt vollen Zugriff auf Aktionen für die Arbeit mit Recovery Readiness (Readiness Check) in ARC. Hängen Sie sie IAM-Benutzern und anderen Principals zu, die vollen Zugriff auf Aktionen zur Wiederherstellung benötigen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonRoute53 RecoveryReadinessFullAccess in der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AmazonRoute 53 RecoveryReadinessReadOnlyAccess

Sie können `AmazonRoute53RecoveryReadinessReadOnlyAccess` an Ihre IAM-Entitäten anhängen. Diese Richtlinie gewährt nur Lesezugriff auf Aktionen für die Arbeit mit Recovery Readiness in ARC. Dies ist nützlich für Benutzer, die den Bereitschaftsstatus und die Konfigurationen der Wiederherstellungsgruppen einsehen müssen. Diese Benutzer können keine Ressourcen zur Wiederherstellungsbereitschaft erstellen, aktualisieren oder löschen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonRoute53 RecoveryReadinessReadOnlyAccess in der Referenz für AWS verwaltete Richtlinien.

Aktualisierungen für AWS verwaltete Richtlinien zur Vorbereitung

Einzelheiten zu den Aktualisierungen der AWS verwalteten Richtlinien für die Bereitschaftsprüfung in ARC seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst finden Sie unterAktualisierungen der AWS verwalteten Richtlinien für Amazon Application Recovery Controller (ARC). Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite ARC-Dokumentenverlauf.

Kontingente für die Bereitschaftsprüfung

Die Bereitschaftsprüfung in Amazon Application Recovery Controller (ARC) unterliegt den folgenden Kontingenten (früher als Limits bezeichnet).

Entität	Kontingent
Anzahl der Wiederherstellungsgruppen pro Konto	5
Anzahl der Zellen pro Konto	15

Entität	Kontingent
Anzahl der verschachtelten Zellen pro Zelle	3
Anzahl der Zellen pro Wiederherstellungsgruppe	3
Anzahl der Ressourcen pro Zelle	10
Anzahl der Ressourcen pro Wiederherstellungsgruppe	10
Anzahl der Ressourcen pro Ressourcensatz	6
Anzahl der Ressourcensätze pro Konto	200
Anzahl der Bereitschaftsprüfungen pro Konto	200
Anzahl der kontoübergreifenden Autorisierungen	100

Codebeispiele für Application Recovery Controller mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Application Recovery Controller mit einem AWS Software Development Kit (SDK) verwendet wird.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Service-Funktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarios anzeigen.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden Sie diesen Dienst mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele

- Grundlegende Beispiele für die Verwendung von Application Recovery Controller AWS SDKs
  - Aktionen für die Verwendung von Application Recovery Controller AWS SDKs
    - Verwenden Sie es GetRoutingControlState mit einem AWS SDK
    - UpdateRoutingControlStateMit einem AWS SDK verwenden

Grundlegende Beispiele für die Verwendung von Application Recovery Controller AWS SDKs

Die folgenden Codebeispiele zeigen, wie Sie die Grundlagen von Amazon Route 53 Application Recovery Controller mit verwenden AWS SDKs.

Beispiele

- Aktionen für die Verwendung von Application Recovery Controller AWS SDKs
  - Verwenden Sie es GetRoutingControlState mit einem AWS SDK
  - UpdateRoutingControlStateMit einem AWS SDK verwenden

Aktionen für die Verwendung von Application Recovery Controller AWS SDKs

Die folgenden Codebeispiele zeigen, wie einzelne Application Recovery Controller-Aktionen mit ausgeführt AWS SDKs werden. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der Amazon Route 53 Application Recovery Controller API-Referenz.

Beispiele

- Verwenden Sie es GetRoutingControlState mit einem AWS SDK
- UpdateRoutingControlStateMit einem AWS SDK verwenden

Verwenden Sie es **`GetRoutingControlState`** mit einem AWS SDK

Die folgenden Code-Beispiele zeigen, wie `GetRoutingControlState` verwendet wird.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public static GetRoutingControlStateResponse
 getRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
             String routingControlArn) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
```

```
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region())).build();
                return client.getRoutingControlState(
                        GetRoutingControlStateRequest.builder()
                                .routingControlArn(routingControlArn).build());
            } catch (Exception exception) {
                System.out.println(exception);
            }
        }
        return null;
    }
```

- Einzelheiten zur API finden Sie GetRoutingControlStatein der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
import boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
```

```
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def get_routing_control_state(routing_control_arn, cluster_endpoints):
    """
    Gets the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.

    :param routing_control_arn: The ARN of the routing control to look up.
    :param cluster_endpoints: The list of cluster endpoints to query.
    :return: The routing control state response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.get_routing_control_state(
                RoutingControlArn=routing_control_arn
            )
            return response
        except Exception as error:
            print(error)
            raise error
```

- Einzelheiten zur API finden Sie GetRoutingControlStatein AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden Sie diesen Dienst mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

UpdateRoutingControlStateMit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `UpdateRoutingControlState` verwendet wird.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public static UpdateRoutingControlStateResponse
 updateRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn,
            String routingControlState) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region()))
                        .build();
                return client.updateRoutingControlState(
                        UpdateRoutingControlStateRequest.builder()

 .routingControlArn(routingControlArn).routingControlState(routingControlState).build());
            } catch (Exception exception) {
```

```
                System.out.println(exception);
            }
        }
        return null;
    }
```

- Einzelheiten zur API finden Sie UpdateRoutingControlStatein der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
import boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def update_routing_control_state(
```

```
    routing_control_arn, cluster_endpoints, routing_control_state
):
    """
    Updates the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.

    :param routing_control_arn: The ARN of the routing control to update the
 state for.
    :param cluster_endpoints: The list of cluster endpoints to try.
    :param routing_control_state: The new routing control state.
    :return: The routing control update response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.update_routing_control_state(
                RoutingControlArn=routing_control_arn,
                RoutingControlState=routing_control_state,
            )
            return response
        except Exception as error:
            print(error)
```

- Einzelheiten zur API finden Sie UpdateRoutingControlStatein AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden Sie diesen Dienst mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Sicherheit im Amazon Application Recovery Controller

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, auf der AWS Dienste in der ausgeführt AWS Cloud werden. 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 Amazon Application Recovery Controller gelten, finden Sie unter AWS Services im Bereich nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, 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 Verwendung von ARC anwenden können. In den folgenden Themen erfahren Sie, wie Sie ARC konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Sie bei der Überwachung und Sicherung Ihrer ARC-Ressourcen unterstützen.

Themen

- Datenschutz in Amazon Application Recovery Controller
- Identity and Access Management für Amazon Application Recovery Controller (ARC)
- Protokollierung und Überwachung in ARC
- Konformitätsprüfung für Amazon Application Recovery Controller
- Ausfallsicherheit im Amazon Application Recovery Controller
- Infrastruktursicherheit in Amazon Application Recovery Controller

Datenschutz in Amazon Application Recovery Controller

Das AWS Modell der mit gilt für den Datenschutz in Amazon Application Recovery Controller. 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 schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- 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 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 ARC oder anderen Geräten arbeiten und dabei die Konsole, die API oder AWS-Services verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie 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

Kundenkonfigurationsinformationen werden in globalen Amazon DynamoDB-Tabellen gespeichert und im Ruhezustand verschlüsselt.

Datensätze, die den Status von Zellen in einem ARC-Cluster enthalten, werden zur Sicherung auf ein Amazon EBS-Volume geschrieben. ARC verwendet die standardmäßige Amazon EBS-Verschlüsselung, während sich die Daten im Ruhezustand befinden.

Verschlüsselung während der Übertragung

Kundenanfragen und -antworten — für die ARC-Konfiguration, Anfragen zum Bereitschaftsstatus, Aktualisierungen des Mobilfunkstatus usw. — werden während der Übertragung während des gesamten Services mithilfe von TLS verschlüsselt.

Identity and Access Management für Amazon Application Recovery Controller (ARC)

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 ARC-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in ARC ausführen.

Dienstbenutzer — Wenn Sie den ARC-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr ARC-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 in ARC nicht auf eine

Funktion zugreifen können, finden Sie weitere Informationen unterFehlerbehebung für -Identität und -Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die ARC-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf ARC. Es ist Ihre Aufgabe, zu bestimmen, auf welche ARC-Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit ARC verwenden kann, finden Sie unterSo funktionieren die Funktionen von Amazon Application Recovery Controller (ARC) mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des Zugriffs auf ARC schreiben können. Beispiele für identitätsbasierte ARC-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien in Amazon Application Recovery Controller (ARC)

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 Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit 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 für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. 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 AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) 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 Methoden für die Übernahme einer Rolle 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 (Verbund) 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - 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 könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. 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 ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

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. Die Berechtigungen in den Richtlinien legen fest, ob eine 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 Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 Inline-Richtlinie wählen, finden Sie unter Auswählen 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.

Zugriffskontrolllisten () ACLs

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

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

Weitere Richtlinientypen

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

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist 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.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) 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 funktionieren die Funktionen von Amazon Application Recovery Controller (ARC) mit IAM

Informationen darüber, wie die einzelnen Funktionen von Amazon Application Recovery Controller (ARC) mit IAM funktionieren, finden Sie in den folgenden Themen:

- IAM für Zonal Shift
- IAM für Zonal Autoshift
- IAM für die Routing-Steuerung
- IAM zur Bereitschaftsprüfung

Beispiele für identitätsbasierte Richtlinien in Amazon Application Recovery Controller (ARC)

Beispiele für identitätsbasierte Richtlinien für jede Funktion in Amazon Application Recovery Controller (ARC) finden Sie in den folgenden Themen in den AWS Identity and Access Management Kapiteln der einzelnen Funktionen:

- Beispiele für identitätsbasierte Richtlinien für zonales Autoshift
- Beispiele für identitätsbasierte Richtlinien für die Zonenverschiebung in ARC

- Beispiele für identitätsbasierte Richtlinien für die Routing-Steuerung in Amazon Application Recovery Controller (ARC)
- Beispiele für identitätsbasierte Richtlinien für die Eignungsprüfung in Amazon Application Recovery Controller (ARC)

AWS verwaltete Richtlinien für Amazon Application Recovery Controller (ARC)

Informationen zu den AWS verwalteten Richtlinien für Funktionen mit verwalteten Richtlinien, einschließlich einer verwalteten Richtlinie für eine dienstbezogene Rolle, finden Sie in den folgenden Themen:

- Verwaltete Richtlinien für zonales Autoshift
- Verwaltete Richtlinien für die Routingsteuerung
- Verwaltete Richtlinien für die Bereitschaftsprüfung

Aktualisierungen der AWS verwalteten Richtlinien für Amazon Application Recovery Controller (ARC)

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Funktionen in ARC an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite ARC-Dokumentenverlauf.

Änderung	Beschreibung	Datum
AWSServiceRoleForPercPracticePolicy— Neue Richtlinie	ARC hat eine neue dienstbezogene Rolle für Autoshift und Übungsläufe hinzugefügt. ARC verwendet die Berechtigungen, die durch die serviceverknüpfte Rolle aktiviert wurden, um vom Kunden bereitgestellte CloudWatch Amazon-Alarme und AWS	30. November 2023

Änderung	Beschreibung	Datum
	Health Dashboard Kundenere ignisse für Übungsläufe zu überwachen und Übungsläufe zu starten. Weitere Informationen über die neue servicebezogene Rolle finden Sie unter. Berechtigungen für dienstver knüpfte Rollen AWSService RoleForZonalAutoshiftPracti ceRun	
AmazonRoute53 RecoveryC ontrolConfigReadOnlyAccess — Aktualisierte Richtlinie	Fügt Berechtigungen für hinzu`GetResourcePolicy` , um die Rückgabe von Details zu AWS Resource Access Manager Ressourcenrichtlin ien für gemeinsam genutzte Ressourcen zu unterstützen.	18. Oktober 2023

Änderung	Beschreibung	Datum

Route53 RecoveryReadinessServiceRolePolicy — Aktualisierte Richtlinie	ARC hat neue Berechtigungen hinzugefügt, um Informationen über EC2 Amazon-Instances abzufragen.
	
	ARC verwendet die folgenden Berechtigungen, um das Abrufen von EC2 Amazon-Instances zu unterstützen, Bereitschaftsprüfungen durchzuführen und den Bereitschaftsstatus für die Instances zu ermitteln.
	
	`ec2:DescribeVpnGateways`
	
	`ec2:DescribeCustomerGateways`
		17. Februar 2023

Änderung	Beschreibung	Datum
Route53 RecoveryReadinessServiceRolePolicy — Aktualisierte Richtlinie	ARC hat eine neue Berechtigung hinzugefügt, um Informationen über Lambda-Funktionen abzufragen. ARC verwendet die folgende Berechtigung, um Informationen über Lambda-Funktionen abzufragen, um Bereitschaftsprüfungen durchzuführen und den Bereitschaftsstatus für die Funktionen zu ermitteln . `lambda:ListProvisionedConcurrencyConfigs`	31. August 2022
AmazonRoute53 RecoveryControlConfigFullAccess — Aktualisierte Richtlinie	Amazon Route 53-Berechtigungen wurden aus der Richtlinie entfernt und ein Hinweis mit den optionalen Berechtigungen hinzugefügt.	26. Mai 2022
AmazonRoute53 RecoveryControlConfigFullAccess — Die Richtlinie wurde aktualisiert	Fehlende erforderliche Amazon Route 53-Berechtigungen wurden zur Richtlinie hinzugefügt.	15. April 2022
AmazonRoute53 RecoveryClusterReadOnlyAccess — Aktualisierte Richtlinie	ARC hat eine neue Berechtigung hinzugefügt`route53-recovery-cluster:ListRoutingControls` , um die Steuerung der Angebotsweiterleitung ARNs mit hoher Verfügbarkeit zu ermöglichen.	15. März 2022

Änderung	Beschreibung	Datum
AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Aktualisierte Richtlinie	ARC hat eine neue Berechtigung hinzugefügt`route53-recovery-control-config:ListTagsForResources` , um das Auflisten von Tags für eine Ressource zu ermöglichen.	20. Dezember 2021
Route53 RecoveryReadinessServiceRolePolicy — Aktualisierte Richtlinie	ARC hat eine neue Berechtigung hinzugefügt, um Informationen über Amazon API Gateway abzufragen. ARC verwendet die Berechtigung,`apigateway:GET` , um Informationen über API Gateway abzufragen, um Bereitschaftsprüfungen durchzuführen und den Bereitschaftsstatus zu ermitteln.	28. Oktober 2021

Änderung	Beschreibung	Datum
AmazonRoute53 RecoveryReadinessReadOnlyAccess — Neue Berechtigungen hinzugefügt	ARC hat AmazonRoute53 zwei neue Berechtigungen hinzugefügtRecoveryReadinessReadOnlyAccess: ARC verwendet `route53-recovery-readiness:GetArchitectureRecommendations` und `route53-recovery-readiness:GetCellReadinessSummary` ermöglicht den schreibgeschützten Zugriff auf diese Aktionen, um mit Wiederherstellungsbereitschaft zu arbeiten.	15. Oktober 2021

Änderung	Beschreibung	Datum

Route53 RecoveryReadinessServiceRolePolicy — Aktualisierte Richtlinie	ARC hat neue Berechtigungen hinzugefügt, um Informationen über Lambda-Funktionen abzufragen.
	
	ARC verwendet die folgenden Berechtigungen, um Informationen über Lambda-Funktionen abzufragen, um Bereitschaftsprüfungen durchzuführen und den Bereitschaftsstatus für diese Funktionen zu ermitteln.
	
	`lambda:GetFunctionConcurrency`
	
	`lambda:GetFunctionConfiguration`
	
	`lambda:GetProvisionedConcurrencyConfig`
	
	`lambda:ListAliases`
	
	`lambda:ListVersionsByFunction`
	
	`lambda:ListEventSourceMappings`
	
	`lambda:ListFunctions`
		8. Oktober 2021

Änderung	Beschreibung	Datum
Route53 RecoveryReadinessServiceRolePolicy — Neue verwaltete Richtlinien hinzugefügt	ARC hat die folgenden neuen verwalteten Richtlinien hinzugefügt: AmazonRoute53 RecoveryReadinessFullAccess AmazonRoute53 RecoveryReadinessReadOnlyAccess AmazonRoute53 RecoveryClusterFullAccess AmazonRoute53 RecoveryClusterReadOnlyAccess AmazonRoute53 RecoveryControlConfigFullAccess AmazonRoute53 RecoveryControlConfigReadOnlyAccess	18. August 2021
ARC hat begonnen, Änderungen zu verfolgen	ARC begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	27. Juli 2021

Fehlerbehebung für -Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon Application Recovery Controller (ARC) und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in ARC durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole

- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine ARC-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in ARC durchzuführen

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `route53-recovery-readiness:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 route53-recovery-readiness:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `route53-recovery-readiness:`*`GetWidget`* zugreifen zu können.

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 ARC 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 ARC 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 ARC-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob ARC diese Funktionen unterstützt, finden Sie unter. So funktionieren die Funktionen von Amazon Application Recovery Controller (ARC) 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Protokollierung und Überwachung in ARC

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Verfügbarkeit und Leistung von ARC und Ihren AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können.

AWS bietet verschiedene Tools zur Überwachung Ihrer ARC-Ressourcen und -Aktivitäten und zur Reaktion auf potenzielle Vorfälle, z. B. AWS CloudTrail und Amazon CloudWatch.

Informationen zur Überwachung der einzelnen Funktionen in ARC finden Sie in den folgenden Themen:

- Protokollierung und Überwachung von Zonenverschiebungen
- Protokollierung und Überwachung für Zonal Autoshift
- Protokollierung und Überwachung zur Routingsteuerung
- Protokollierung und Überwachung zur Überprüfung der Einsatzbereitschaft

Konformitätsprüfung für Amazon Application Recovery Controller

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon Application Recovery Controller im Rahmen mehrerer AWS Compliance-Programme. Zu diesen Programmen gehören SOC, PCI, HIPAA und andere.

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.

- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Ausfallsicherheit im Amazon Application Recovery Controller

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet ARC mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

Infrastruktursicherheit in Amazon Application Recovery Controller

Als verwalteter Service ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf ARC zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme 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.

Dokumentverlauf für das Amazon Application Recovery Controller (ARC) Developer Guide

Die folgenden Einträge beschreiben wichtige Änderungen, die an der Amazon Application Recovery Controller (ARC) -Dokumentation vorgenommen wurden.

- Version: neueste
- Letzte Aktualisierung der Dokumentation: 26. März 2025

Änderung	Beschreibung	Datum
Testen Sie ARC Zonal Autoshift mit AWS FIS	Sie können AWS FIS damit testen, wie ARC Zonal Autoshift Ihre Anwendung während einer AZ-Stromunterbrechung automatisch wiederherstellt Weitere Informationen finden Sie unter Zonal Autoshift testen mit. AWS FIS	26. März 2025
ARC unterstützt jetzt IPv6 Endpunkte für Routing-Steuerung und Zonenverschiebung.	ARC unterstützt jetzt IPv6 Endpunkte für Routing-Steuerungen und Zonenverschiebungen. Weitere Informationen finden Sie unter Routing-Steuerungskomponenten einrichten.	21. November 2024
Zonenverschiebungsfunktion für Amazon EC2 Auto Scaling Scaling-Gruppen	ARC unterstützt jetzt Zonal Shift für Amazon EC2 Auto Scaling Scaling-Gruppen.	18. November 2024

Änderung	Beschreibung	Datum
	Weitere Informationen finden Sie unter Support für Amazon EC2 Auto Scaling Scaling-Gruppen.	
Zonenverschiebungsfähigkeit für Amazon EKS	Sie können eine Zonenverschiebung für einen Amazon EKS-Cluster starten, oder Sie können es für Sie AWS übernehmen lassen, indem Sie Zonal Autoshift aktivieren. Diese Verschiebung aktualisiert den Fluss des east-to-west Netzwerkverkehrs in Ihrem Cluster, sodass nur Netzwerkendpunkte für Pods berücksichtigt werden, die auf Worker-Knoten ausgeführt werden, die fehlerfrei sind. AZs Weitere Informationen finden Sie unter Support für Amazon Elastic Kubernetes Service.	22. Oktober 2024
Zonale Shift-Funktion für Network Load Balancer	ARC unterstützt jetzt Zonal Shift für Network Load Balancer mit zonenübergreifenden aktivierten oder zonenübergreifenden deaktivierten Konfigurationen. Weitere Informationen finden Sie unter Support für Network Load Balancer.	11. Oktober 2024

Änderung	Beschreibung	Datum
Autoshift-Observer-Benachrichtigungen	Mit Autoshift-Observer-Benachrichtigungen können Sie zonales Autoshift so konfigurieren, dass Sie über Amazon benachrichtigt werden, wenn ein Autoshift AWS gestartet wird EventBridge, um den Verkehr von einer potenziell beeinträchtigten Availability Zone weg zu verlagern. Sie müssen keine bestimmten Ressourcen mit zonalem Autoshift konfigurieren, um diese separaten Benachrichtigungen zu aktivieren. Weitere Informationen finden Sie unter Zonal Autoshift mit Amazon verwenden. EventBridge	12. Juli 2024

Änderung	Beschreibung	Datum
Reorganisation der Dokumente nach den einzelnen Funktionen	Organisiert den Inhalt des Entwicklerhandbuchs neu, sodass er in untergeordnete Entwicklerhandbücher aufgeteilt wird. Das heißt, es gibt jetzt separate Abschnitte, die umfassende Informationen zu den einzelnen Funktionen in ARC enthalten: Zonal Shift und Zonal Autoshift für Multi-AZ-Recovery sowie Routing-Steuerung und Bereitschaftsprüfung für Multi-Region-Recovery. Weitere Informationen finden Sie unter Was ist Amazon Application Recovery Controller (ARC).	30. April 2024
Fügt zonale Autoshift-Fähigkeit hinzu	Fügt eine neue Funktion in ARC hinzu, mit der Sie autorisieren AWS , den Ressourcenverkehr für eine Anwendung in Ihrem Namen aus einer Availability Zone zu verlagern, um die Zeit bis zur Wiederherstellung bei Ereignissen zu verkürzen. Weitere Informationen finden Sie unter Zonal Autoshift in Amazon Application Recovery Controller (ARC).	30. November 2023

Änderung	Beschreibung	Datum
Fügt eine neue serviceverknüpfte Rolle hinzu	Fügt eine neue dienstbezogene Rolle für zonale AWSServiceRoleForZonalAutoshiftPracticeRunAutoshift-Übungsläufe hinzu. Weitere Informationen finden Sie unter Berechtigungen von serviceverknüpften Rollen für AWSServiceRoleForZonalAutoshiftPracticeRun.	30. November 2023
Fügt kontenübergreifende Unterstützung für Cluster hinzu	Fügt kontenübergreifende Unterstützung für Cluster in ARC mit hinzu AWS Resource Access Manager, sodass Sie einfach und sicher einen Cluster verwenden können, um Control Panels und Routing-Steuerelemente zu hosten, die mehreren verschiedenen AWS Konten gehören. Weitere Informationen finden Sie unter Kontoübergreifende Support für Cluster in ARC.	18. Oktober 2023

Änderung	Beschreibung	Datum
Aktualisiert eine verwaltete Richtlinie	Aktualisiert die `AmazonRoute53RecoveryControlConfigReadOnly` verwaltete Richtlinie `eGetResourcePolicy` , um Berechtigungen für hinzuzufügen und die Rückgabe von Details zu AWS Resource Access Manager Ressourcenrichtlinien für gemeinsam genutzte Ressourcen zu unterstützen. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien.	19. September 2023
Die serviceverknüpfte Rolle wurde aktualisiert	Neue Berechtigungen wurden hinzugefügt `ec2:DescribeVpnGateways` und `ec2:DescribeCustomerGateways` der serviceverknüpften Rolle für ARC wurde die Unterstützung für das Abrufen von EC2 Amazon-Instances hinzugefügt. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für ARC.	17. Februar 2023

Änderung	Beschreibung	Datum
GA-Version für Zonal Shift	Unterstützt die GA-Version von Zonal Shift for ARC, die eine attributebasierte Zugriffskontrolle (ABAC) für verwaltete Ressourcen beinhaltet, die in ARC für Zonal Shift registriert sind. Weitere Informationen finden Sie unter Attributbasierte Zugriffskontrolle (ABAC) mit ARC.	10. Januar 2023
Neue Multi-AZ-Zonenverschiebung hinzugefügt	Inhalt hinzugefügt, der einen neuen Dienst in ARC, Zonal Shift, für Multi-AZ-Anwendungen beschreibt. Sie können eine Zonenverschiebung starten, um den Verkehr für eine Load Balancer-Ressource vorübergehend von einer Availability Zone weg zu verlagern. Weitere Informationen finden Sie unter Zonal Shift in ARC.	28. November 2022

Änderung	Beschreibung	Datum
Die serviceverknüpfte Rolle wurde aktualisiert	Der serviceverknüpften Rolle wurde eine neue Berechtigung hinzugefügt `lambda:ListProvisionedConcurrencyConfigs` , damit ARC Informationen über Lambda-Funktionen abfragen kann. Weitere Informationen finden Sie unter Verwenden von dienstbezogenen Rollen für ARC.	31. August 2022
Verwaltete Richtlinie aktualisiert	Die `AmazonRoute53RecoveryControlConfigFullAccess` verwaltete Richtlinie wurde aktualisiert, um Amazon Route 53-Berechtigungen zu entfernen und sie als optional aufzulisten. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Amazon Application Recovery Controller (ARC).	26. Mai 2022

Änderung	Beschreibung	Datum
Verwaltete Richtlinie aktualisiert	Die `AmazonRoute53RecoveryControlConfigFullAccess` verwaltete Richtlinie wurde aktualisiert, sodass sie die erforderlichen Amazon Route 53-Berechtigungen enthält. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Amazon Application Recovery Controller (ARC).	15. April 2022
CLI-Beispiel für die neue List Routing Controls API hinzugefügt	Es wurden ein Beispiel für einen CLI-Befehl und Empfehlungen für bewährte Methoden für den neuen API-Betrieb zur Listenrouting-Steuerung hinzugefügt, der in der äußerst zuverlässigen ARC-Datenebene-API enthalten ist. Weitere Informationen finden Sie unter Auflisten und Aktualisieren von Routingsteuerungen und Status.	31. März 2022

Änderung	Beschreibung	Datum
Unterstützung für das Überschreiben von Sicherheitsregeln wurde hinzugefügt	Es wurde Unterstützung für das Überschreiben von Sicherheitsregeln hinzugefügt, sodass Sie Schutzmaßnahmen für die Routingsteuerung umgehen können, die mit von Ihnen konfigurierten Sicherheitsregeln durchgesetzt werden. Das Außerkrafttsetzen von Sicherheitsregeln kann beispielsweise in einem Szenario mit Glasbruch während eines Failovers für die Notfallwiederherstellung erforderlich sein. Weitere Informationen finden Sie unter Sicherheitsregeln außer Kraft setzen, um den Verkehr umzuleiten.	2. März 2022
Zusätzliche Tagging-Unterstützung hinzugefügt	Unterstützung für das Taggen zusätzlicher Ressourcen in ARC wurde hinzugefügt, einschließlich Clustern, Bedienfeldern, Routing-Steuerelementen und Sicherheitsregeln. Weitere Informationen finden Sie unter Tagging in Amazon Application Recovery Controller (ARC).	20. Dezember 2021

Änderung	Beschreibung	Datum
Verwaltete Richtlinie aktualisiert	Die `AmazonRoute53RecoveryControlConfigReadOnly` verwaltete Richtlinie wurde aktualisiert, um die Berechtigung zum Auflisten von Tags für eine Ressource hinzuzufügen. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Amazon Application Recovery Controller (ARC)	20. Dezember 2021
Unterstützung für Echtzeitwarnungen hinzugefügt mit EventBridge	Unterstützung für hinzugefügt. Das bedeutet EventBridge, dass Sie jetzt Regeln hinzufügen können, um Benachrichtigungen zu erhalten und auf Statusänderungen der ARC-Bereitschaftsprüfung zu reagieren, z. B. wenn sich ein Status von READY auf NOT READY ändert. Weitere Informationen finden Sie unter Verwenden von ARC mit Amazon EventBridge.	20. Dezember 2021

Änderung	Beschreibung	Datum
Es wurden Beispiele für Statuscodes zur Routing-Steuerung hinzugefügt	Es wurden Codebeispiele hinzugefügt, um zu veranschaulichen, wie Cluster-Endpunkte nacheinander ausprobiert werden, wenn Sie API-Operationen verwenden, um den Status der Routing-Steuerung abzurufen oder zu aktualisieren. Weitere Informationen finden Sie unter API-Beispiele für Amazon Application Recovery Controller (ARC).	16. November 2021
Einer Nur-Lese-Richtlinie wurden neue Berechtigungen hinzugefügt	Der Richtlinie wurden zwei neue Berechtigungen hinzugefügt`AmazonRoute53RecoveryReadinessReadOnlyAccess` : `route53-recovery-readiness:GetArchitectureRecommendations` und. `route53-recovery-readiness:GetCellReadinessSummary` Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Amazon Application Recovery Controller (ARC).	9. November 2021

Änderung	Beschreibung	Datum
Unterstützung für den Amazon API Gateway Gateway-Ressourcentyp hinzugefügt	Ein neuer Ressourcentyp, Amazon API Gateway, wurde hinzugefügt und die mit dem ARC-Dienst verknüpften Rollenberechtigungen aktualisiert, sodass ARC API Gateway mit Bereitschaftsprüfungen prüfen kann. Weitere Informationen finden Sie unter Bereitschaftsregeln und unterstützte Ressourcentypen und Verwenden von serviceverknüpften Rollen für ARC.	28. Oktober 2021
Unterstützung für den Ressourcentyp Lambda-Funktionen hinzugefügt	Ein neuer Ressourcentyp, Lambda-Funktionen, wurde hinzugefügt und die mit dem ARC-Dienst verknüpften Rollenberechtigungen aktualisiert, sodass ARC Lambda-Funktionen mit Bereitschaftsprüfungen prüfen kann. Weitere Informationen finden Sie unter Bereitschaftsregeln und unterstützte Ressourcentypen und Verwenden von dienstbezogenen Rollen für ARC.	8. Oktober 2021

Änderung	Beschreibung	Datum
Links zu CloudFormation und Terraform-Vorlagen hinzugefügt	Es wurden Links zu herunterladbaren AWS CloudFormation und Hashicorp-Terraform-Vorlagen hinzugefügt, um Ihnen den schnellen Einstieg in die Verwendung von ARC zu erleichtern. Weitere Informationen finden Sie unter Wiederherstellungsbereitschaft mit einer neuen Anwendung.	13. September 2021

Änderung	Beschreibung	Datum
Neue verwaltete Richtlinien hinzugefügt	Die folgenden AWS verwaltet en Richtlinien für ARC wurden hinzugefügt: `AmazonRou te53RecoveryReadin essFullAccess` `AmazonRoute53Recov eryReadinessReadOn lyAccess` `AmazonRou te53Recov eryClusterFullAcce ss` ,,`AmazonRou te53Recov eryClusterReadOnly Access` ,`AmazonRou te53RecoveryContro lConfigFullAccess` , und`AmazonRoute53Recov eryControlConfigRe adOnlyAccess` . Weitere Informationen finden Sie unter AWS Verwaltet e Richtlinien für Amazon Application Recovery Controlle r (ARC).	18. August 2021

Änderung	Beschreibung	Datum
Die Nachverfolgung AWS verwalteter Richtlinien für Amazon Application Recovery Controller (ARC) wurde gestartet	Aktualisierungen für verwaltete Richtlinien werden ab dem Datum der ersten Veröffentlichung nachverfolgt. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Amazon Application Recovery Controller (ARC).	27. Juli 2021
Erste Version von Amazon Application Recovery Controller (ARC)	ARC verbessert die Anwendungsverfügbarkeit durch die zentrale Koordination von Failovers innerhalb einer AWS Region oder über mehrere Regionen hinweg. ARC bietet Bereitschaftsprüfungen, um sicherzustellen, dass Ihre Anwendungen für den Failover-Verkehr skaliert und für die Umgehung von Ausfällen konfiguriert sind. Darüber hinaus bietet es eine äußerst zuverlässige Routingsteuerung, sodass Sie Anwendungen wiederherstellen können, indem Sie den Datenverkehr beispielsweise zwischen Availability Zones oder Regionen umleiten. Weitere Informationen finden Sie unter Was ist ARC? .	27. Juli 2021

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.