AWS Well-Architected Framework

Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud

Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud: AWS Well-Architected Framework

Table of Contents

Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud

Datum der Veröffentlichung: 12. Februar 2021 () Dokumentverlauf

Disaster Recovery ist der Prozess der Vorbereitung auf eine Katastrophe und der Wiederherstellung nach einer Katastrophe. Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt, wird als Katastrophe betrachtet. In diesem paper werden die bewährten Methoden für die Planung und das Testen der Notfallwiederherstellung für jeden Workload beschrieben, für den bereitgestellt wird AWS, und es werden verschiedene Ansätze zur Risikominderung und zur Einhaltung der Recovery Time Objective (RTO) und Recovery Point Objective (RPO) für diesen Workload vorgestellt.

In diesem Whitepaper wird beschrieben, wie Sie Disaster Recovery für Workloads auf implementieren können. AWS Informationen zur Verwendung AWS als Disaster Recovery-Standort AWS für lokale Workloads finden Sie unter Disaster Recovery of On-Premises-Anwendungen.

Einführung

Ihr Workload muss die vorgesehene Funktion korrekt und konsistent erfüllen. Um dies zu erreichen, müssen Sie Ihre Architektur auf Ausfallsicherheit ausrichten. Resilienz ist die Fähigkeit eines Workloads, sich nach Infrastruktur-, Service- oder Anwendungsunterbrechungen zu erholen, Rechenressourcen dynamisch zu erwerben, um den Bedarf zu decken, und Störungen wie Fehlkonfigurationen oder vorübergehende Netzwerkprobleme zu minimieren.

Disaster Recovery (DR) ist ein wichtiger Bestandteil Ihrer Resilienzstrategie und befasst sich damit, wie Ihre Arbeitslast im Notfall reagiert (ein Notfall ist ein Ereignis, das schwerwiegende negative Auswirkungen auf Ihr Unternehmen hat). Diese Reaktion muss auf den Geschäftszielen Ihres Unternehmens basieren, in denen die Strategie Ihres Workloads zur Vermeidung von Datenverlusten (Recovery Point Objective, RPO) und zur Reduzierung von Ausfallzeiten, wenn Ihr Workload nicht zur Verfügung steht, festgelegt wird, das sogenannte Recovery Time Objective (RTO). Sie müssen daher bei der Gestaltung Ihrer Workloads in der Cloud Resilienz implementieren, um Ihre Wiederherstellungsziele (RPO und RTO) für ein bestimmtes einmaliges Katastrophenereignis zu erreichen. Dieser Ansatz hilft Ihrem Unternehmen, die Geschäftskontinuität im Rahmen der Business Continuity Planning (BCP) aufrechtzuerhalten.

Dieses paper konzentriert sich auf die Planung, den Entwurf und die Implementierung von Architekturen, AWS die die Disaster Recovery-Ziele Ihres Unternehmens erfüllen. Die hier bereitgestellten Informationen richten sich an Personen in technologischer Position, wie z. B. Chief Technology Officers (CTOs), Architekten, Entwickler, Mitglieder des Betriebsteams und Personen, die mit der Bewertung und Minderung von Risiken beauftragt sind.

Notfallwiederherstellung und Verfügbarkeit

Disaster Recovery kann mit Verfügbarkeit verglichen werden, was ein weiterer wichtiger Bestandteil Ihrer Resilienzstrategie ist. Während bei der Notfallwiederherstellung die Ziele für einmalige Ereignisse gemessen werden, werden bei Verfügbarkeitszielen Mittelwerte über einen bestimmten Zeitraum gemessen.

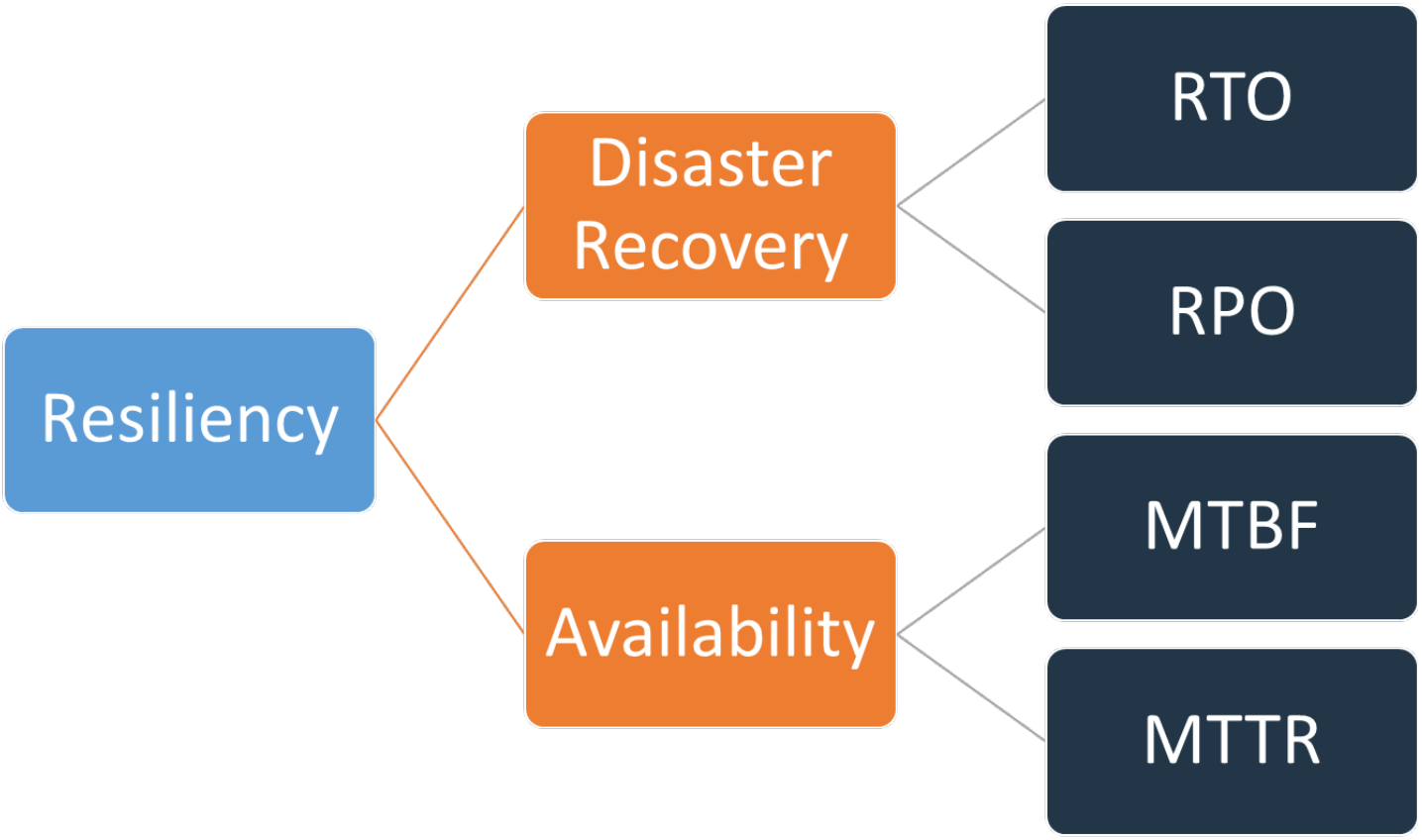

Abbildung 1: Resilienzziele

Die Verfügbarkeit wird anhand der Mean Time Between Failures (MTBF) und der Mean Time to Recover (MTTR) berechnet:

$$Availability = \frac{Available\ for\ Use\ Time}{Total\ Time} = \frac{MTBF}{MTBF + MTTR}$$

Dieser Ansatz wird oft als „neun“ bezeichnet, wohingegen ein Verfügbarkeitsziel von 99,9% als „drei Neunen“ bezeichnet wird.

Für Ihren Workload ist es möglicherweise einfacher, erfolgreiche und fehlgeschlagene Anfragen zu zählen, anstatt einen zeitbasierten Ansatz zu verwenden. In diesem Fall kann die folgende Berechnung verwendet werden:

$$Availability = \frac{Successful\ Responses}{Valid\ Requests}$$

Disaster Recovery konzentriert sich auf Notfallereignisse, wohingegen sich Verfügbarkeit auf häufigere Störungen kleineren Ausmaßes wie Komponentenausfälle, Netzwerkprobleme, Softwarefehler und Lastspitzen konzentriert. Das Ziel der Notfallwiederherstellung ist die Geschäftskontinuität, wohingegen es bei der Verfügbarkeit darum geht, die Zeit zu maximieren, in der ein Workload zur Ausführung seiner beabsichtigten Geschäftsfunktionen verfügbar ist. Beides sollte Teil Ihrer Resilienzstrategie sein.

Sind Sie Well-Architected?

Das AWS Well-Architected Framework hilft Ihnen dabei, die Vor- und Nachteile der Entscheidungen zu verstehen, die Sie beim Aufbau von Systemen in der Cloud treffen. Die sechs Säulen des Frameworks ermöglichen es Ihnen, bewährte Architekturpraktiken für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme kennenzulernen. Mit dem AWS Well-Architected Tool, das kostenlos in der AWS-Managementkonsole verfügbar ist, können Sie Ihre Workloads anhand dieser bewährten Methoden überprüfen, indem Sie für jede Säule eine Reihe von Fragen beantworten.

Die in diesem Whitepaper behandelten Konzepte erweitern die bewährten Methoden des Whitepapers zur Säule der Zuverlässigkeit, insbesondere die Frage REL 13, „Wie planen Sie die Notfallwiederherstellung (DR)?“. Nachdem Sie die Methoden in diesem Whitepaper implementiert haben, sollten Sie Ihren Workload mit dem AWS Well-Architected Tool überprüfen (oder erneut überprüfen).

Modell der geteilten Verantwortung für Ausfallsicherheit

Ausfallsicherheit ist eine gemeinsame AWS Verantwortung von Ihnen, dem Kunden. Es ist wichtig, dass Sie verstehen, wie Disaster Recovery und Verfügbarkeit als Teil der Ausfallsicherheit im Rahmen dieses gemeinsamen Modells funktionieren.

AWS-Verantwortung „Resilienz der Cloud“

AWS ist für die Ausfallsicherheit der Infrastruktur verantwortlich, auf der alle in der AWS-Cloud angebotenen Services ausgeführt werden. Diese Infrastruktur umfasst die Hardware, Software, Netzwerke und Einrichtungen, die AWS-Cloud-Services ausführen. AWS unternimmt wirtschaftlich vertretbare Anstrengungen, um diese AWS-Cloud-Services verfügbar zu machen, und stellt sicher, dass die Verfügbarkeit der Services die AWS-Service Level Agreements (SLAs) erfüllt oder übertrifft.

Die globale Cloud-Infrastruktur von AWS wurde entwickelt, um Kunden den Aufbau hochbelastbarer Workload-Architekturen zu ermöglichen. Jede AWS-Region ist vollständig isoliert und besteht aus mehreren Availability Zones, bei denen es sich um physisch isolierte Infrastrukturpartitionen handelt. Availability Zones isolieren Fehler, die die Ausfallsicherheit von Workloads beeinträchtigen könnten, und verhindern, dass sie sich auf andere Zonen in der Region auswirken. Gleichzeitig sind jedoch alle Zonen in einer AWS-Region über Netzwerke mit hoher Bandbreite und niedriger Latenz über vollständig redundante, dedizierte Metro-Glasfasern miteinander verbunden, sodass Netzwerke mit hohem Durchsatz und niedriger Latenz zwischen den Zonen bereitgestellt werden. Der gesamte Datenverkehr zwischen den Zonen ist verschlüsselt. Die Leistung des Netzwerks ist ausreichend, um eine synchrone Replikation zwischen den Zonen zu ermöglichen. Wenn eine Anwendung auf mehrere Bereiche aufgeteilt wird AZs, sind Unternehmen besser isoliert und vor Problemen wie Stromausfällen, Blitzeinschlägen, Tornados, Wirbelstürmen und mehr geschützt.

Kundenverantwortung „Resilienz in der Cloud“

Ihre Verantwortung richtet sich nach den AWS-Cloud-Services, die Sie auswählen. Dies bestimmt den Umfang der Konfigurationsarbeit, die Sie als Teil Ihrer Verantwortung für die Ausfallsicherheit durchführen müssen. Bei einem Service wie Amazon Elastic Compute Cloud (Amazon EC2) muss der Kunde beispielsweise alle erforderlichen Aufgaben zur Konfiguration und Verwaltung der Ausfallsicherheit ausführen. Kunden, die EC2 Amazon-Instances einsetzen, sind dafür verantwortlich, EC2 Instances an mehreren Standorten (wie AWS Availability Zones) bereitzustellen, Selbstheilung mithilfe von Services wie Amazon EC2 Auto Scaling zu implementieren und bewährte Methoden

für die robuste Workload-Architektur für Anwendungen zu verwenden, die auf den Instances installiert sind. Bei verwalteten Services wie Amazon S3 und Amazon DynamoDB betreibt AWS die Infrastrukturebene, das Betriebssystem und die Plattformen, und Kunden greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Sie sind dafür verantwortlich, die Ausfallsicherheit Ihrer Daten zu verwalten, einschließlich Sicherungs-, Versionsverwaltungs- und Replikationsstrategien.

Die Bereitstellung Ihres Workloads in mehreren Availability Zones in einer AWS-Region ist Teil einer Hochverfügbarkeitsstrategie, die darauf abzielt, Workloads zu schützen, indem Probleme in einer Availability Zone isoliert werden und die Redundanz der anderen Availability Zones genutzt wird, um weiterhin Anfragen zu bearbeiten. Eine Multi-AZ-Architektur ist außerdem Teil einer Notfallwiederherstellungsstrategie, die darauf abzielt, Workloads besser zu isolieren und vor Problemen wie Stromausfällen, Blitzeinschlägen, Tornados, Erdbeben und anderen Ereignissen zu schützen. DR-Strategien können auch mehrere AWS-Regionen nutzen. In einer aktiven/passiven Konfiguration führt der Service für den Workload beispielsweise ein Failover von seiner aktiven Region in seine DR-Region durch, wenn die aktive Region keine Anfragen mehr bearbeiten kann.

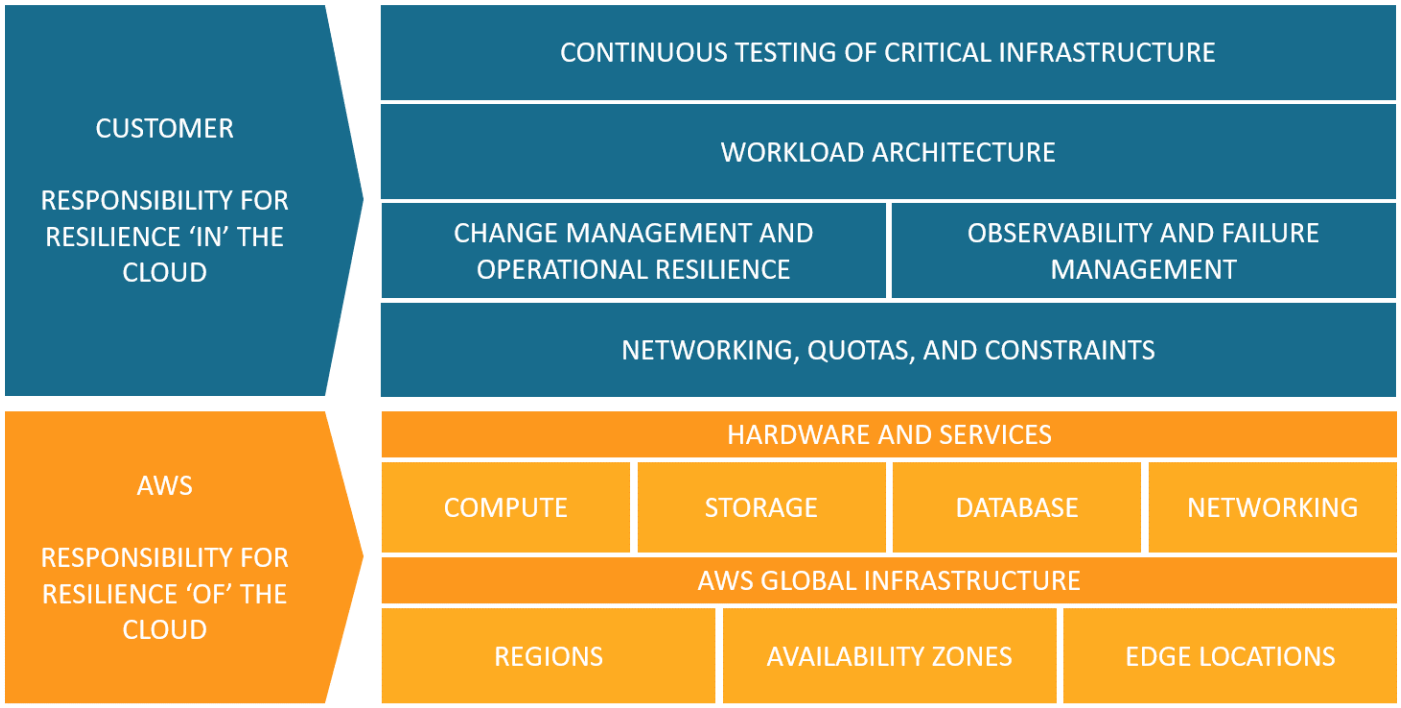

Abbildung 2: Ausfallsicherheit ist eine gemeinsame Verantwortung von AWS und dem Kunden

Was ist eine Katastrophe?

Bei der Planung der Notfallwiederherstellung sollten Sie Ihren Plan für die folgenden drei Hauptkategorien von Katastrophen berücksichtigen:

- Naturkatastrophen wie Erdbeben oder Überschwemmungen
- Technische Ausfälle wie Stromausfall oder Netzwerkkonnektivität
- Menschliche Handlungen, wie z. B. unbeabsichtigte Fehlkonfigurationen oder der Zugriff oder die Änderung durch unauthorized/outside Parteien

Jede dieser potenziellen Katastrophen wird auch geografische Auswirkungen haben, die lokal, regional, landesweit, kontinental oder global sein können. Sowohl die Art der Katastrophe als auch die geografischen Auswirkungen sind wichtig, wenn Sie Ihre Notfallwiederherstellungsstrategie in Betracht ziehen. Sie können beispielsweise ein lokales Überschwemmungsproblem, das zu einem Ausfall des Rechenzentrums führt, durch den Einsatz einer Multi-AZ-Strategie abmildern, da davon nicht mehr als eine Availability Zone betroffen wäre. Bei einem Angriff auf Produktionsdaten müssten Sie jedoch eine Notfallwiederherstellungsstrategie anwenden, bei der ein Failover auf Backup-Daten in einer anderen AWS-Region durchgeführt wird.

Hochverfügbarkeit ist keine Notfallwiederherstellung

Sowohl Verfügbarkeit als auch Disaster Recovery basieren auf einigen der gleichen bewährten Methoden, wie z. B. der Überwachung auf Ausfälle, der Bereitstellung an mehreren Standorten und dem automatischen Failover. Verfügbarkeit konzentriert sich jedoch auf Komponenten des Workloads, wohingegen sich Disaster Recovery auf einzelne Kopien des gesamten Workloads konzentriert. Die Notfallwiederherstellung verfolgt andere Ziele als die Verfügbarkeit, d. h. die Messung der Zeit bis zur Wiederherstellung nach größeren Ereignissen, die als Katastrophen gelten. Sie sollten zunächst sicherstellen, dass Ihr Workload Ihren Verfügbarkeitszielen entspricht, da Sie mit einer hochverfügbaren Architektur die Anforderungen Ihrer Kunden bei Ereignissen erfüllen können, die sich auf die Verfügbarkeit auswirken. Ihre Disaster-Recovery-Strategie erfordert andere Ansätze als die für die Verfügbarkeit. Der Schwerpunkt liegt auf der Bereitstellung diskreter Systeme an mehreren Standorten, sodass Sie bei Bedarf die gesamte Arbeitslast ausfallsicher abwickeln können.

Bei der Planung der Notfallwiederherstellung müssen Sie die Verfügbarkeit Ihrer Arbeitslast berücksichtigen, da sich dies auf Ihren Ansatz auswirkt. Ein Workload, der auf einer einzelnen EC2 Amazon-Instance in einer Availability Zone ausgeführt wird, hat keine hohe Verfügbarkeit. Wenn sich ein lokales Hochwasserproblem auf diese Availability Zone auswirkt, erfordert dieses Szenario einen Failover zu einer anderen AZ, um die DR-Ziele zu erreichen. Vergleichen Sie dieses Szenario mit einem hochverfügbaren Workload, der an mehreren Standorten aktiv/aktiv bereitgestellt wird, wobei der Workload in mehreren aktiven Regionen bereitgestellt wird und alle Regionen den Produktionsdatenverkehr bedienen. Selbst in dem unwahrscheinlichen Fall, dass eine Region aufgrund einer schweren Katastrophe unbrauchbar wird, wird die DR-Strategie dadurch erreicht, dass der gesamte Datenverkehr an die verbleibenden Regionen weitergeleitet wird.

Die Art und Weise, wie Sie mit Daten umgehen, unterscheidet sich auch zwischen Verfügbarkeit und Notfallwiederherstellung. Stellen Sie sich eine Speicherlösung vor, die kontinuierlich an einen anderen Standort repliziert, um eine hohe Verfügbarkeit zu erreichen (z. B. eine active/active Workload an mehreren Standorten). Wenn eine oder mehrere Dateien auf dem primären Speichergerät gelöscht oder beschädigt werden, können diese zerstörerischen Änderungen auf das sekundäre Speichergerät repliziert werden. In diesem Szenario ist trotz hoher Verfügbarkeit die Möglichkeit eines Failovers im Falle einer Datenlöschung oder -beschädigung beeinträchtigt. Stattdessen ist im Rahmen einer DR-Strategie auch ein point-in-time Backup erforderlich.

Plan zur Geschäftskontinuität (BCP)

Ihr Notfallwiederherstellungsplan sollte Teil des Business Continuity Plans (BCP) Ihres Unternehmens sein und kein eigenständiges Dokument sein. Es hat keinen Sinn, aggressive Disaster-Recovery-Ziele für die Wiederherstellung eines Workloads beizubehalten, wenn die Geschäftsziele dieses Workloads aufgrund der Auswirkungen der Katastrophe auf andere Bereiche Ihres Unternehmens als Ihren Workload nicht erreicht werden können. Ein Erdbeben könnte Sie beispielsweise daran hindern, Produkte zu transportieren, die Sie in Ihrer E-Commerce-Anwendung gekauft haben. Selbst wenn eine effektive Notfallwiederherstellung dafür sorgt, dass Ihr Workload funktioniert, muss Ihr BCP den Transportanforderungen gerecht werden. Ihre DR-Strategie sollte auf den Geschäftsanforderungen, Prioritäten und dem Kontext basieren.

Analyse der Auswirkungen auf das Geschäft und Risikobewertung

Eine Analyse der Geschäftsauswirkungen sollte die geschäftlichen Auswirkungen einer Unterbrechung Ihrer Workloads quantifizieren. Dabei sollte ermittelt werden, welche Auswirkungen es auf interne und externe Kunden hat, wenn Sie Ihre Workloads nicht nutzen können, und welche Auswirkungen dies auf Ihr Unternehmen hat. Die Analyse sollte dabei helfen, festzustellen, wie schnell die Arbeitslast verfügbar gemacht werden muss und wie viel Datenverlust toleriert werden kann. Es ist jedoch wichtig zu beachten, dass Wiederherstellungsziele nicht isoliert festgelegt werden sollten. Die Wahrscheinlichkeit einer Unterbrechung und die Kosten der Wiederherstellung sind wichtige Faktoren, anhand derer der geschäftliche Nutzen einer Notfallwiederherstellung für einen Workload ermittelt werden kann.

Die Auswirkungen auf das Geschäft können zeitabhängig sein. Möglicherweise sollten Sie erwägen, dies bei Ihrer Notfallwiederherstellungsplanung zu berücksichtigen. Beispielsweise hat eine Störung Ihres Gehaltsabrechnungssystems wahrscheinlich sehr starke Auswirkungen auf das Unternehmen, kurz bevor alle bezahlt werden, aber sie können nur geringe Auswirkungen haben, wenn alle bereits bezahlt wurden.

Anhand einer Risikobewertung der Art der Katastrophe und der geografischen Auswirkungen sowie eines Überblicks über die technische Umsetzung Ihres Workloads wird für jede Art von Katastrophe die Wahrscheinlichkeit einer Störung ermittelt.

Bei sehr kritischen Workloads könnten Sie die Bereitstellung einer Infrastruktur in mehreren Regionen mit Datenreplikation und kontinuierlichen Backups in Betracht ziehen, um die Auswirkungen auf Ihr Geschäft zu minimieren. Für weniger kritische Workloads besteht eine gültige Strategie

möglicherweise darin, überhaupt keine Notfallwiederherstellung einzurichten. Und für einige Katastrophenszenarien ist es auch sinnvoll, keine Notfallwiederherstellungsstrategie zu haben, da eine fundierte Entscheidung auf der Grundlage einer geringen Wahrscheinlichkeit des Eintretens der Katastrophe getroffen wird. Denken Sie daran, dass Availability Zones innerhalb einer AWS-Region bereits mit einem angemessenen Abstand zwischen ihnen und einer sorgfältigen Standortplanung entworfen wurden, sodass sich die häufigsten Katastrophen nur auf eine Zone auswirken und nicht auf die anderen. Daher erfüllt eine Multi-AZ-Architektur innerhalb einer AWS-Region möglicherweise bereits einen Großteil Ihrer Anforderungen an die Risikominderung.

Die Kosten der Disaster Recovery-Optionen sollten bewertet werden, um sicherzustellen, dass die Disaster-Recovery-Strategie unter Berücksichtigung der geschäftlichen Auswirkungen und Risiken den richtigen Geschäftswert bietet.

Mit all diesen Informationen können Sie die Bedrohung, das Risiko, die Auswirkungen und die Kosten verschiedener Notfallszenarien und die damit verbundenen Wiederherstellungsoptionen dokumentieren. Diese Informationen sollten verwendet werden, um Ihre Wiederherstellungsziele für jede Ihrer Workloads zu bestimmen.

Wiederherstellungsziele (RTO und RPO)

Bei der Entwicklung einer Disaster Recovery (DR) -Strategie berücksichtigen Unternehmen in der Regel die Ziele Recovery Time Objective (RTO) und Recovery Point Objective (RPO).

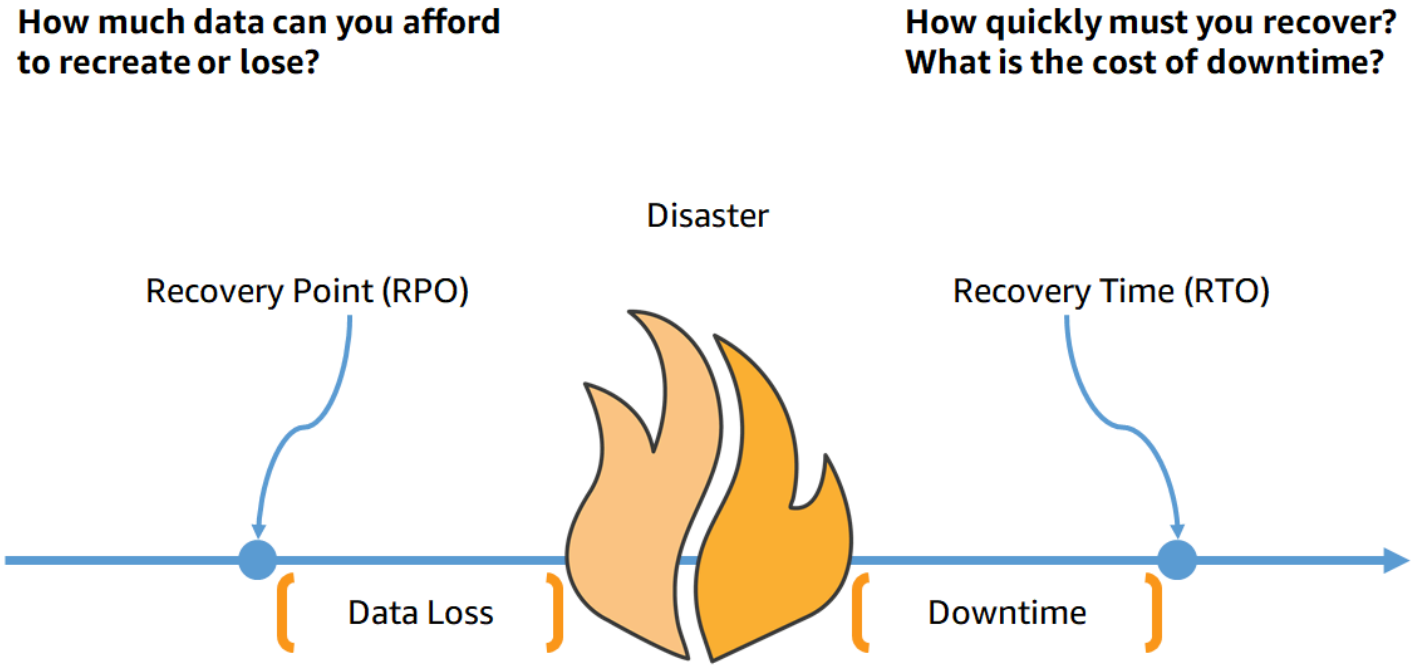

Abbildung 3: Wiederherstellungsziele

Das Recovery Time Objective (RTO) ist die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes. Dieses Ziel bestimmt, welches Zeitfenster als akzeptables Zeitfenster angesehen wird, wenn der Service nicht verfügbar ist, und wird von der Organisation festgelegt.

In diesem paper werden im Großen und Ganzen vier DR-Strategien erörtert: Backup und Wiederherstellung, Pilotbetrieb, Warm-Standby und Multi-Site active/active (siehe Disaster Recovery-Optionen in der Cloud). In der folgenden Abbildung hat das Unternehmen seinen maximal zulässigen RTO sowie den Grenzwert festgelegt, den es für seine Strategie zur Wiederherstellung der Dienste ausgeben kann. Angesichts der Unternehmensziele erfüllen die DR-Strategien Pilot Light oder Warm Standby sowohl die RTO- als auch die Kostenkriterien.

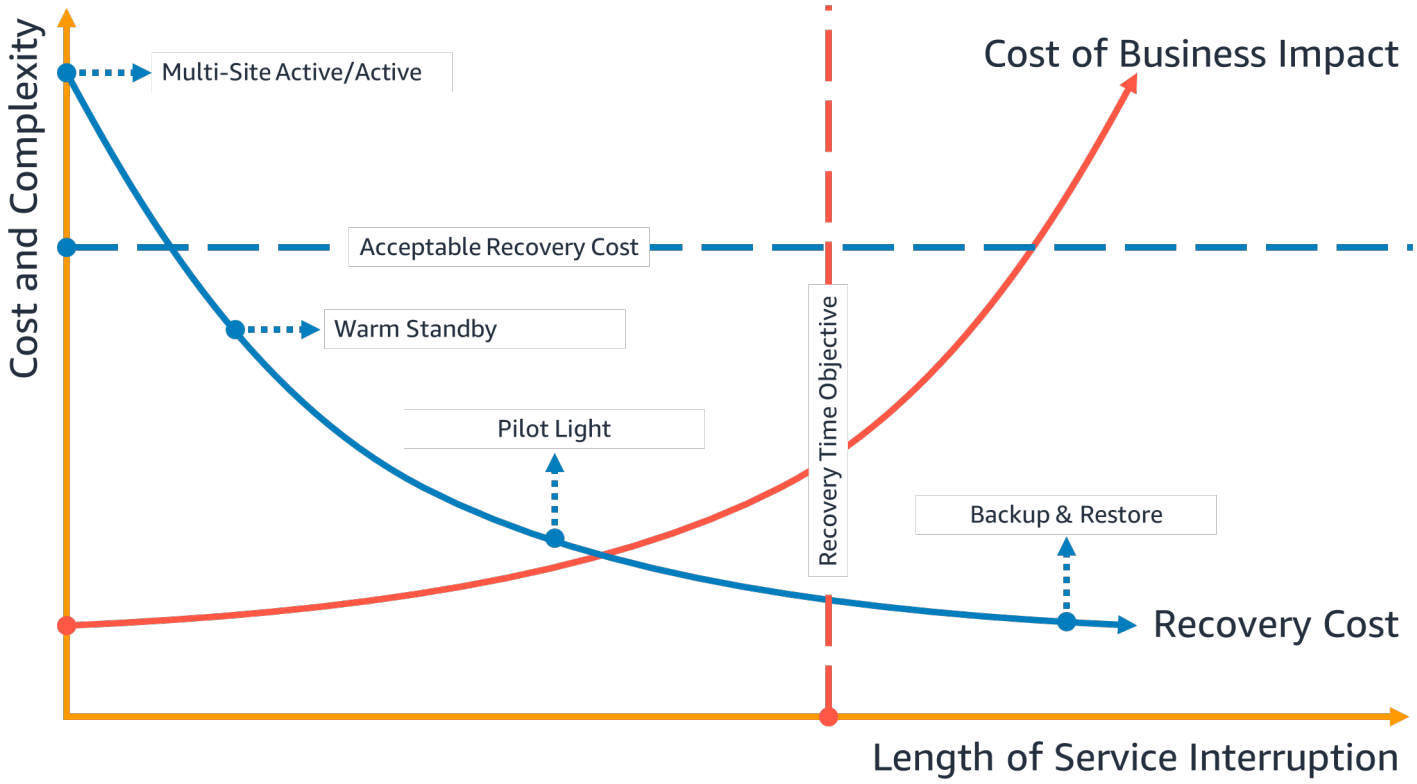

Abbildung 4: Ziel der Wiederherstellungszeit

Das Recovery Point Objective (RPO) ist die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dieses Ziel bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Recovery Point und der Betriebsunterbrechung angesehen wird, und wird von der Organisation festgelegt.

In der folgenden Abbildung hat das Unternehmen sein maximal zulässiges RPO sowie die Obergrenze der Ausgaben für seine Datenwiederherstellungsstrategie festgelegt. Von den vier DR-Strategien erfüllen entweder die DR-Strategie Pilot Light oder die Warm Standby DR-Strategie beide Kriterien in Bezug auf RPO und Kosten.

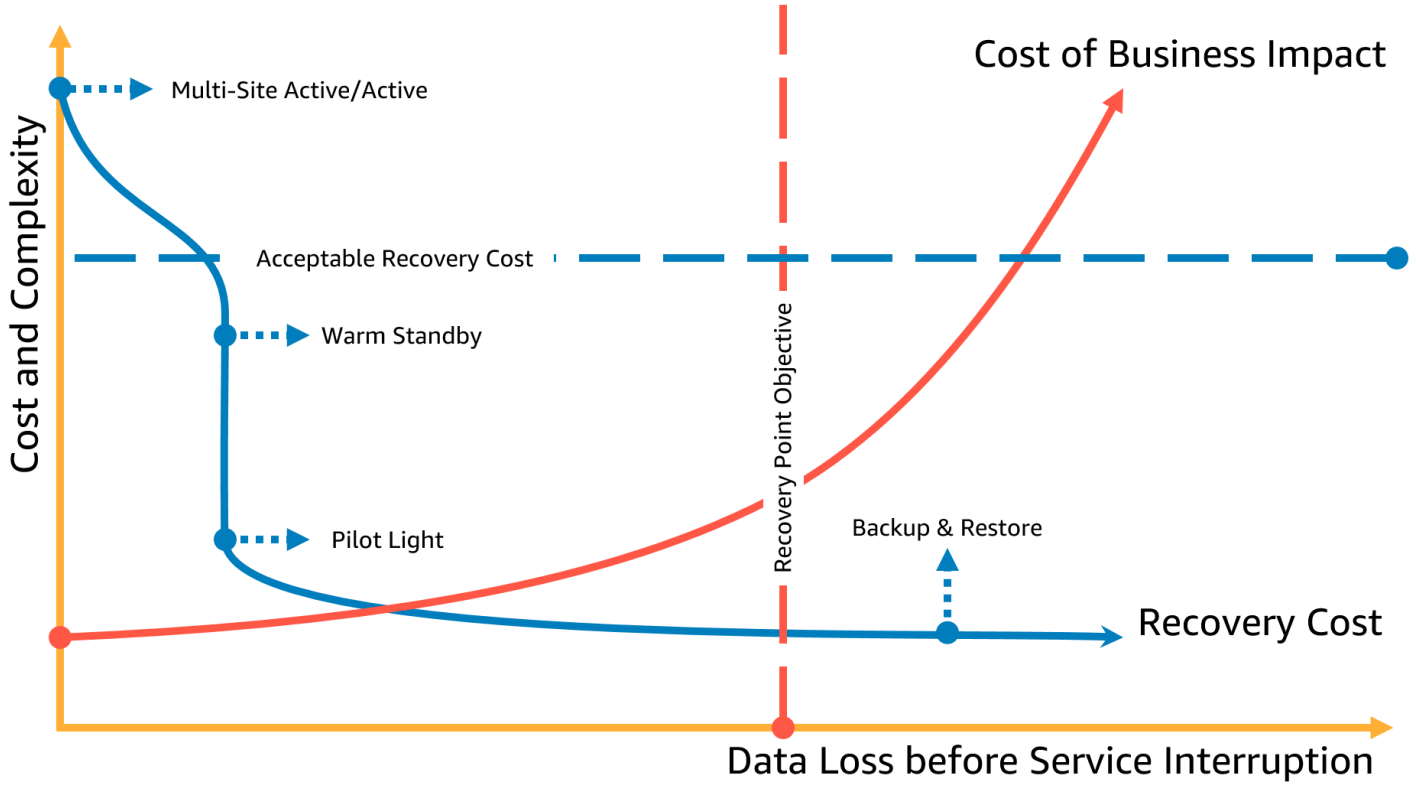

Abbildung 5: Ziel des Wiederherstellungspunkts

> **Note**
>
> Wenn die Kosten der Wiederherstellungsstrategie höher sind als die Kosten des Ausfalls oder Verlusts, sollte die Wiederherstellungsoption nicht eingeführt werden, es sei denn, es gibt einen sekundären Grund, wie z. B. gesetzliche Anforderungen. Berücksichtigen Sie bei dieser Bewertung Wiederherstellungsstrategien mit unterschiedlichen Kosten.

Die Notfallwiederherstellung in der Cloud unterscheidet sich

Disaster-Recovery-Strategien entwickeln sich mit technischen Innovationen weiter. Ein Disaster-Recovery-Plan vor Ort kann den physischen Transport von Bändern oder die Replikation von Daten an einen anderen Standort beinhalten. Ihr Unternehmen muss die geschäftlichen Auswirkungen, Risiken und Kosten seiner bisherigen Disaster Recovery-Strategien neu bewerten, um seine DR-Ziele auf AWS zu erreichen. Die Notfallwiederherstellung in der AWS-Cloud bietet die folgenden Vorteile gegenüber herkömmlichen Umgebungen:

- Schnelle Wiederherstellung nach einem Notfall mit reduzierter Komplexität
- Einfache und wiederholbare Tests ermöglichen es Ihnen, einfacher und häufiger zu testen
- Ein geringerer Verwaltungsaufwand verringert die betriebliche Belastung
- Möglichkeiten zur Automatisierung verringern das Fehlerrisiko und verkürzen die Wiederherstellungszeit

Mit AWS können Sie die festen Investitionskosten eines physischen Backup-Rechenzentrums gegen die variablen Betriebskosten einer geeigneten Umgebung in der Cloud eintauschen, wodurch die Kosten erheblich gesenkt werden können.

Für viele Unternehmen basierte die lokale Notfallwiederherstellung auf dem Risiko einer Unterbrechung einer oder mehrerer Workloads in einem Rechenzentrum und der Wiederherstellung von gesicherten oder replizierten Daten in einem sekundären Rechenzentrum. Wenn Unternehmen Workloads auf AWS bereitstellen, können sie einen gut strukturierten Workload implementieren und sich auf das Design der globalen AWS-Cloud-Infrastruktur verlassen, um die Auswirkungen solcher Störungen abzumildern. Weitere Informationen zu bewährten Architekturmethoden für die Entwicklung und den Betrieb zuverlässiger, sicherer, effizienter und kostengünstiger Workloads in der Cloud finden Sie im Whitepaper AWS Well-Architected Framework — Reliability Pillar. Verwenden Sie das AWS Well-Architected Tool, um Ihre Workloads regelmäßig zu überprüfen, um sicherzustellen, dass sie den Best Practices und Richtlinien des Well-Architected Framework entsprechen. Das Tool ist kostenlos im verfügbar. AWS Management Console

Wenn sich Ihre Workloads auf AWS befinden, müssen Sie sich keine Gedanken über die Konnektivität des Rechenzentrums (mit Ausnahme Ihrer Zugriffsmöglichkeiten), Stromversorgung, Klimatisierung, Brandbekämpfung und Hardware machen. All dies wird für Sie verwaltet und Sie haben Zugriff auf mehrere fehlerisolierte Availability Zones (die jeweils aus einem oder mehreren diskreten Rechenzentren bestehen).

Einzelne AWS-Region

Bei einem Katastrophenfall, der auf einer Unterbrechung oder dem Verlust eines physischen Rechenzentrums beruht, trägt die Implementierung eines hochverfügbaren Workloads in mehreren Availability Zones innerhalb einer einzigen AWS-Region dazu bei, natürliche und technische Katastrophen zu vermeiden. Durch die kontinuierliche Sicherung von Daten innerhalb dieser einzelnen Region kann das Risiko menschlicher Bedrohungen wie Fehler oder unbefugte Aktivitäten, die zu Datenverlust führen könnten, verringert werden. Jede AWS-Region besteht aus mehreren Availability Zones, die jeweils von Fehlern in den anderen Zonen isoliert sind. Jede Availability Zone besteht wiederum aus einem oder mehreren diskreten physischen Rechenzentren. Um schwerwiegende Probleme besser zu isolieren und eine hohe Verfügbarkeit zu erreichen, können Sie Workloads auf mehrere Zonen in derselben Region partitionieren. Availability Zones sind auf physische Redundanz ausgelegt und bieten Stabilität, sodass auch bei Stromausfällen, Internetausfällen, Überschwemmungen und anderen Naturkatastrophen eine unterbrechungsfreie Leistung gewährleistet ist. Unter AWS Global Cloud Infrastructure erfahren Sie, wie AWS das macht.

Durch die Bereitstellung in mehreren Availability Zones in einer einzigen AWS-Region ist Ihr Workload besser vor dem Ausfall eines einzelnen (oder sogar mehrerer) Rechenzentren geschützt. Für zusätzliche Sicherheit bei Ihrer Bereitstellung in einer Region können Sie Daten und Konfigurationen (einschließlich der Infrastrukturdefinition) in einer anderen Region sichern. Diese Strategie reduziert den Umfang Ihres Notfallwiederherstellungsplans, sodass er nur noch Datensicherung und -wiederherstellung umfasst. Die Nutzung der Resilienz mehrerer Regionen durch die Sicherung in einer anderen AWS-Region ist im Vergleich zu den anderen im folgenden Abschnitt beschriebenen Optionen für mehrere Regionen einfach und kostengünstig. Wenn Sie beispielsweise ein Backup auf Amazon Simple Storage Service (Amazon S3) erstellen, haben Sie Zugriff auf den sofortigen Abruf Ihrer Daten. Wenn Ihre DR-Strategie für Teile Ihrer Daten jedoch lockerere Anforderungen an die Abrufzeiten (von Minuten bis Stunden) vorsieht, können Sie mit Amazon S3 Glacier oder Amazon S3 Glacier Deep Archive die Kosten Ihrer Sicherungs- und Wiederherstellungsstrategie erheblich senken.

Für einige Workloads gelten möglicherweise gesetzliche Anforderungen an den Speicherort der Daten. Wenn dies auf Ihren Workload an einem Standort zutrifft, der derzeit nur über eine AWS-Region verfügt, können Sie nicht nur Multi-AZ-Workloads für hohe Verfügbarkeit wie oben beschrieben entwerfen, sondern auch die AZs innerhalb dieser Region als separate Standorte verwenden, was hilfreich sein kann, um die für Ihren Workload in dieser Region geltenden Datenresidenzanforderungen zu erfüllen. Die in den folgenden Abschnitten beschriebenen DR-

Strategien verwenden mehrere AWS-Regionen, können aber auch mithilfe von Availability Zones anstelle von Regionen implementiert werden.

Mehrere AWS-Regionen

Bei einem Katastrophenfall, bei dem das Risiko besteht, dass mehrere Rechenzentren in großer Entfernung voneinander verloren gehen, sollten Sie Notfallwiederherstellungsoptionen in Betracht ziehen, um natürliche und technische Katastrophen zu vermeiden, die eine ganze Region innerhalb von AWS betreffen. Alle in den folgenden Abschnitten beschriebenen Optionen können als multiregionale Architekturen implementiert werden, um vor solchen Katastrophen zu schützen.

Optionen für die Notfallwiederherstellung in der Cloud

Disaster Recovery-Strategien, die Ihnen innerhalb von AWS zur Verfügung stehen, lassen sich grob in vier Ansätze einteilen, die von den niedrigen Kosten und der geringen Komplexität der Erstellung von Backups bis hin zu komplexeren Strategien mit mehreren aktiven Regionen reichen. Active/passive Strategien verwenden einen aktiven Standort (z. B. eine AWS-Region), um den Workload zu hosten und den Datenverkehr bereitzustellen. Die passive Site (z. B. eine andere AWS-Region) wird für die Wiederherstellung verwendet. Die passive Site stellt keinen aktiven Datenverkehr bereit, bis ein Failover-Ereignis ausgelöst wird.

Es ist wichtig, Ihre Disaster-Recovery-Strategie regelmäßig zu überprüfen und zu testen, damit Sie sie im Bedarfsfall auch anwenden können. Verwenden Sie AWS Resilience Hub, um die Widerstandsfähigkeit Ihrer AWS Workloads kontinuierlich zu überprüfen und zu verfolgen, einschließlich der Frage, ob Sie Ihre RTO- und RPO-Ziele voraussichtlich erreichen werden.

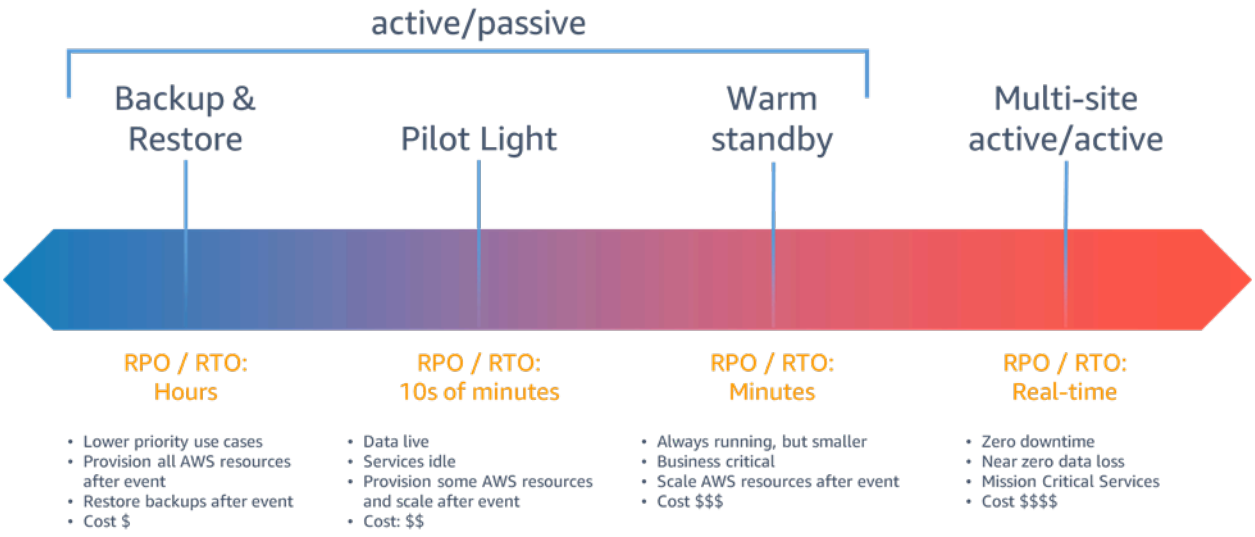

Abbildung 6: Strategien für die Notfallwiederherstellung

Bei einem Notfall, der auf einer Unterbrechung oder dem Verlust eines physischen Rechenzentrums für eine gut strukturierte, hochverfügbare Arbeitslast beruht, benötigen Sie möglicherweise nur einen Sicherungs- und Wiederherstellungsansatz für die Notfallwiederherstellung. Wenn Ihre Definition eines Notfalls über die Unterbrechung oder den Verlust eines physischen Rechenzentrums hinaus auf das einer Region hinausgeht oder wenn Sie gesetzlichen Anforderungen unterliegen, die dies erfordern, sollten Sie Pilot Light, Warm Standby oder Multi-Site Active/Active in Betracht ziehen.

Denken Sie bei der Auswahl Ihrer Strategie und der AWS-Ressourcen für deren Implementierung daran, dass wir innerhalb von AWS Services üblicherweise in die Datenebene und die Kontrollebene unterteilen. Die Datenebene ist zuständig für die Bereitstellung von Echtzeitservices, während die Steuerebene dazu verwendet wird, die Umgebung zu konfigurieren. Für maximale Ausfallsicherheit sollten Sie im Rahmen Ihres Failover-Vorgangs nur Datenebenenoperationen verwenden. Dies liegt daran, dass für die Datenebenen in der Regel eine höhere Verfügbarkeit als für die Steuerungsebenen vorgesehen ist.

Backup und Backup

Backup und Wiederherstellung sind ein geeigneter Ansatz, um Datenverlust oder -beschädigung zu verhindern. Dieser Ansatz kann auch zur Abwehr regionaler Katastrophen verwendet werden, indem Daten in andere AWS-Regionen repliziert werden, oder um fehlende Redundanz für Workloads zu verringern, die in einer einzigen Availability Zone bereitgestellt werden. Zusätzlich zu den Daten müssen Sie die Infrastruktur, die Konfiguration und den Anwendungscode in der Wiederherstellungsregion erneut bereitstellen. Damit die Infrastruktur schnell und ohne Fehler neu bereitgestellt werden kann, sollten Sie bei der Bereitstellung stets Infrastructure as Code (IaC) verwenden und Dienste wie AWS CloudFormationoder den verwenden. AWS Cloud Development Kit (AWS CDK) Ohne IaC kann die Wiederherstellung von Workloads in der Wiederherstellungsregion komplex sein, was zu längeren Wiederherstellungszeiten und möglicherweise zu einer Überschreitung Ihres RTO-Werts führen kann. Stellen Sie sicher, dass Sie neben den Benutzerdaten auch Code und Konfiguration sichern, einschließlich Amazon Machine Images (AMIs), die Sie zum Erstellen von EC2 Amazon-Instances verwenden. Sie können AWS CodePipelinees verwenden, um die erneute Bereitstellung von Anwendungscode und Konfiguration zu automatisieren.

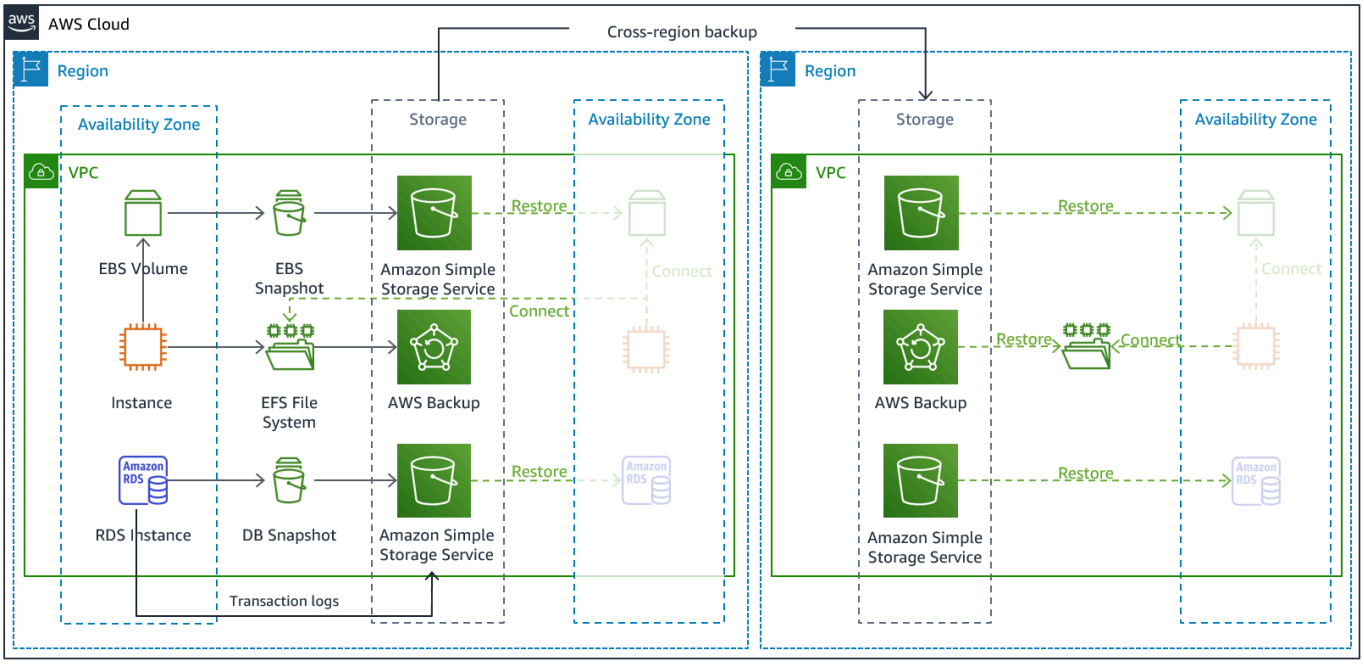

Abbildung 7: Architektur für Backup und Wiederherstellung

AWS-Services

Für Ihre Workload-Daten ist eine Backup-Strategie erforderlich, die regelmäßig oder kontinuierlich ausgeführt wird. Wie oft Sie Ihr Backup ausführen, bestimmt Ihren erreichbaren Wiederherstellungspunkt (der sich an Ihrem RPO orientieren sollte). Das Backup sollte auch eine Möglichkeit bieten, es auf den Zeitpunkt zurückzusetzen, an dem es erstellt wurde. Backup mit point-in-time Wiederherstellung ist über die folgenden Dienste und Ressourcen verfügbar:

- Snapshot von Amazon Elastic Block Store (Amazon EBS)
- Amazon DynamoDB-Backup
- Amazon RDS-Snapshot
- Amazon Aurora Aurora-DB-Snapshot
- Amazon EFS-Backup (bei Verwendung AWS Backup)
- Amazon Redshift Redshift-Snapshot
- Amazon Neptune Neptune-Schnappschuss
- Amazon DocumentDB
- Amazon FSx für Windows File Server, Amazon FSx für Lustre, Amazon FSx für NetApp ONTAP und Amazon FSx für OpenZFS

Für Amazon Simple Storage Service (Amazon S3) können Sie Amazon S3 Cross-Region Replication (CRR) verwenden, um Objekte kontinuierlich asynchron in einen S3-Bucket in der DR-Region zu kopieren und gleichzeitig eine Versionierung für die gespeicherten Objekte bereitzustellen, sodass Sie Ihren Wiederherstellungspunkt wählen können. Die kontinuierliche Replikation von Daten hat den Vorteil, dass sie die kürzeste Zeit (nahe Null) für die Sicherung Ihrer Daten bietet, schützt aber möglicherweise nicht vor Katastrophenereignissen wie Datenbeschädigung oder böswilligen Angriffen (z. B. unberechtigtes Löschen von Daten) sowie vor point-in-time Backups. Kontinuierliche Replikation wird im Abschnitt AWS-Services für Pilot Light behandelt.

AWS Backupbietet einen zentralen Ort für die Konfiguration, Planung und Überwachung der AWS-Backup-Funktionen für die folgenden Services und Ressourcen:

- Volumen im Amazon Elastic Block Store (Amazon EBS)
- EC2Amazon-Instanzen
- Amazon Relational Database Service (Amazon RDS) -Datenbanken (einschließlich Amazon Aurora Aurora-Datenbanken)
- Amazon DynamoDB-Tabellen
- Dateisysteme von Amazon Elastic File System (Amazon EFS)
- AWS Storage Gateway-Volumes
- Amazon FSx für Windows File Server, Amazon FSx für Lustre, Amazon FSx für NetApp ONTAP und Amazon FSx für OpenZFS

AWS Backup unterstützt das Kopieren von Backups zwischen Regionen, z. B. in eine Region für die Notfallwiederherstellung.

Als zusätzliche Strategie zur Notfallwiederherstellung für Ihre Amazon S3 S3-Daten aktivieren Sie die Versionierung von S3-Objekten. Die Objektversionierung schützt Ihre Daten in S3 vor den Folgen von Lösch- oder Änderungsaktionen, indem die ursprüngliche Version vor der Aktion beibehalten wird. Die Objektversionierung kann ein nützliches Mittel zur Abmilderung von Katastrophen sein, die auf menschliches Versagen zurückzuführen sind. Wenn Sie die S3-Replikation verwenden, um Daten in Ihrer DR-Region zu sichern, fügt Amazon S3 standardmäßig nur im Quell-Bucket eine Löschmarkierung hinzu, wenn ein Objekt im Quell-Bucket gelöscht wird. Dieser Ansatz schützt Daten in der DR-Region vor böswilligen Löschungen in der Quellregion.

Zusätzlich zu den Daten müssen Sie auch die Konfiguration und Infrastruktur sichern, die für die erneute Bereitstellung Ihres Workloads und die Einhaltung Ihres Recovery Time Objective (RTO)

erforderlich sind. AWS CloudFormationstellt Infrastructure as Code (IaC) bereit und ermöglicht es Ihnen, alle AWS-Ressourcen in Ihrem Workload zu definieren, sodass Sie sie zuverlässig für mehrere AWS-Konten und AWS-Regionen bereitstellen und erneut bereitstellen können. Sie können EC2 Amazon-Instances, die von Ihrem Workload verwendet werden, als Amazon Machine Images (AMIs) sichern. Das AMI wird aus Snapshots des Root-Volumes Ihrer Instance und aller anderen EBS-Volumes erstellt, die an Ihre Instance angehängt sind. Sie können dieses AMI verwenden, um eine wiederhergestellte Version der EC2 Instance zu starten. Ein AMI kann innerhalb oder zwischen Regionen kopiert werden. Sie können es auch verwenden, AWS Backupum Backups zwischen Konten und in andere AWS-Regionen zu kopieren. Die kontoübergreifende Backup-Funktion trägt zum Schutz vor Katastrophenereignissen bei, zu denen auch Insiderbedrohungen oder Kontokompromittierungen gehören. AWS Backup fügt außerdem zusätzliche EC2 Backup-Funktionen hinzu — zusätzlich zu den einzelnen EBS-Volumes der Instanz speichert und verfolgt es die folgenden Metadaten: Instanztyp, konfigurierte Virtual Private Cloud (VPC), Sicherheitsgruppe, IAM-Rolle, Überwachungskonfiguration und Tags. AWS Backup Diese zusätzlichen Metadaten werden jedoch nur verwendet, wenn das EC2 Backup in derselben AWS-Region wiederhergestellt wird.

Alle Daten, die in der Disaster Recovery-Region als Backups gespeichert sind, müssen zum Zeitpunkt des Failovers wiederhergestellt werden. AWS Backup bietet Wiederherstellungsfunktionen, ermöglicht derzeit jedoch keine geplante oder automatische Wiederherstellung. Sie können die automatische Wiederherstellung in der DR-Region mithilfe des AWS-SDK auf Anfrage APIs implementieren AWS Backup. Sie können dies als regelmäßig wiederkehrenden Job einrichten oder die Wiederherstellung auslösen, wenn ein Backup abgeschlossen ist. Die folgende Abbildung zeigt ein Beispiel für die automatische Wiederherstellung mithilfe von Amazon Simple Notification Service (Amazon SNS) und AWS Lambda. Die Implementierung einer geplanten regelmäßigen Datenwiederherstellung ist eine gute Idee, da es sich bei der Datenwiederherstellung aus dem Backup um einen Vorgang auf der Kontrollebene handelt. Wenn dieser Vorgang während eines Notfalls nicht verfügbar wäre, hätten Sie immer noch funktionsfähige Datenspeicher, die aus einer kürzlich durchgeführten Sicherung erstellt wurden.

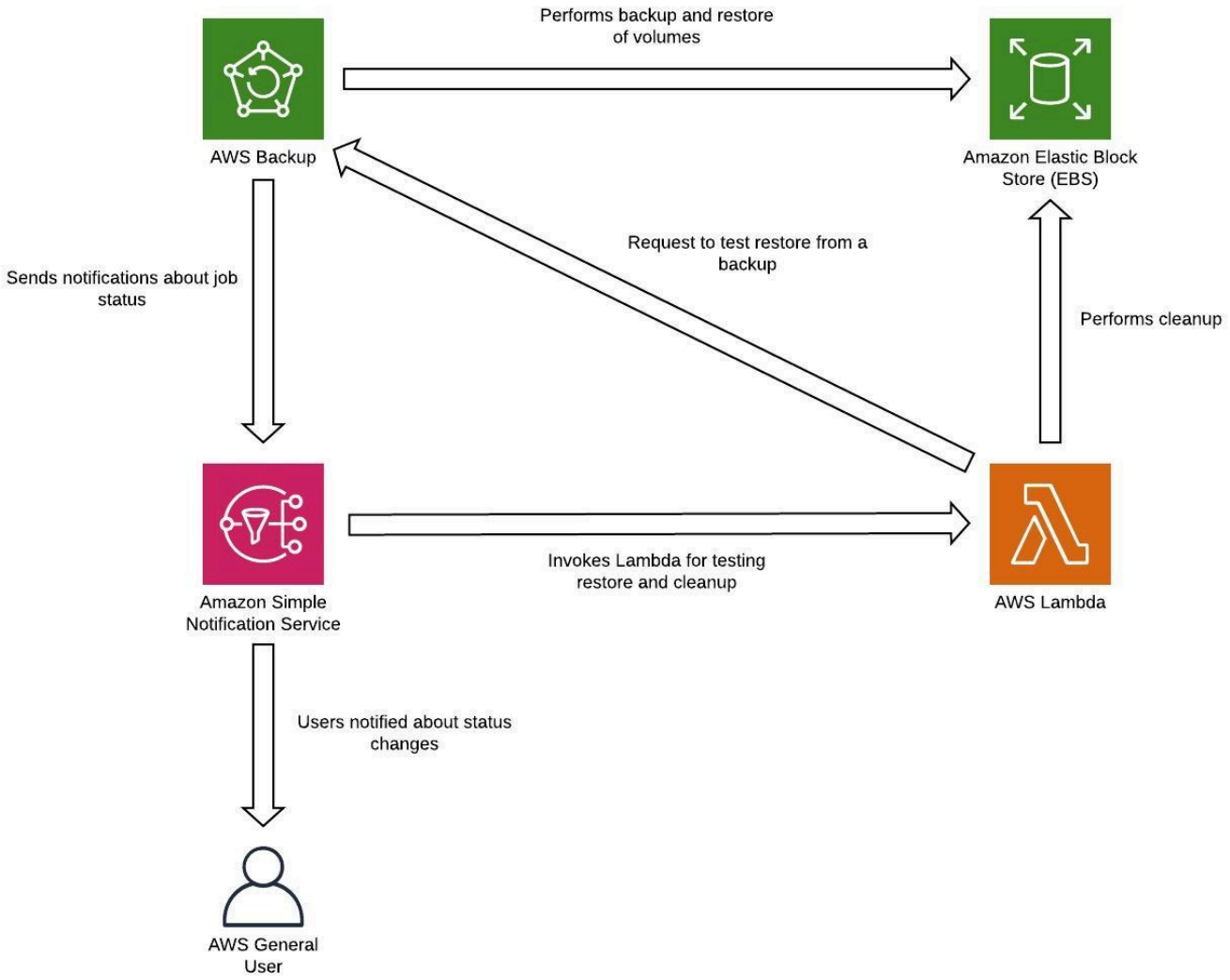

Abbildung 8: Backups wiederherstellen und testen

> **Note**
>
> Ihre Backup-Strategie muss das Testen Ihrer Backups beinhalten. Weitere Informationen finden Sie im Abschnitt Testen der Notfallwiederherstellung. Eine praktische Demonstration der Implementierung finden Sie im AWS Well-Architected Lab: Testing Backup and Restore of Data.

Pilot light

Beim Pilot-Light-Ansatz replizieren Sie Ihre Daten von einer Region in eine andere und stellen eine Kopie Ihrer zentralen Workload-Infrastruktur bereit. Ressourcen, die zur Unterstützung der Datenreplikation und -sicherung erforderlich sind, wie Datenbanken und Objektspeicher, sind immer eingeschaltet. Andere Elemente, wie z. B. Anwendungsserver, enthalten zwar Anwendungscode und Konfigurationen, sind jedoch „ausgeschaltet“ und werden nur beim Testen oder beim Auslösen eines Disaster Recovery-Failovers verwendet. In der Cloud haben Sie die Flexibilität, Ressourcen zu deprovisionieren, wenn Sie sie nicht benötigen, und sie dann bereitzustellen, wenn Sie sie benötigen. Eine bewährte Methode bei ausgeschaltetem System besteht darin, die Ressource nicht bereitzustellen und dann die Konfiguration und die Funktionen zu erstellen, um sie bei Bedarf bereitzustellen („einzuschalten“). Im Gegensatz zum Sicherungs- und Wiederherstellungsansatz ist Ihre Kerninfrastruktur immer verfügbar und Sie haben jederzeit die Möglichkeit, schnell eine vollständige Produktionsumgebung bereitzustellen, indem Sie Ihre Anwendungsserver einschalten und skalieren.

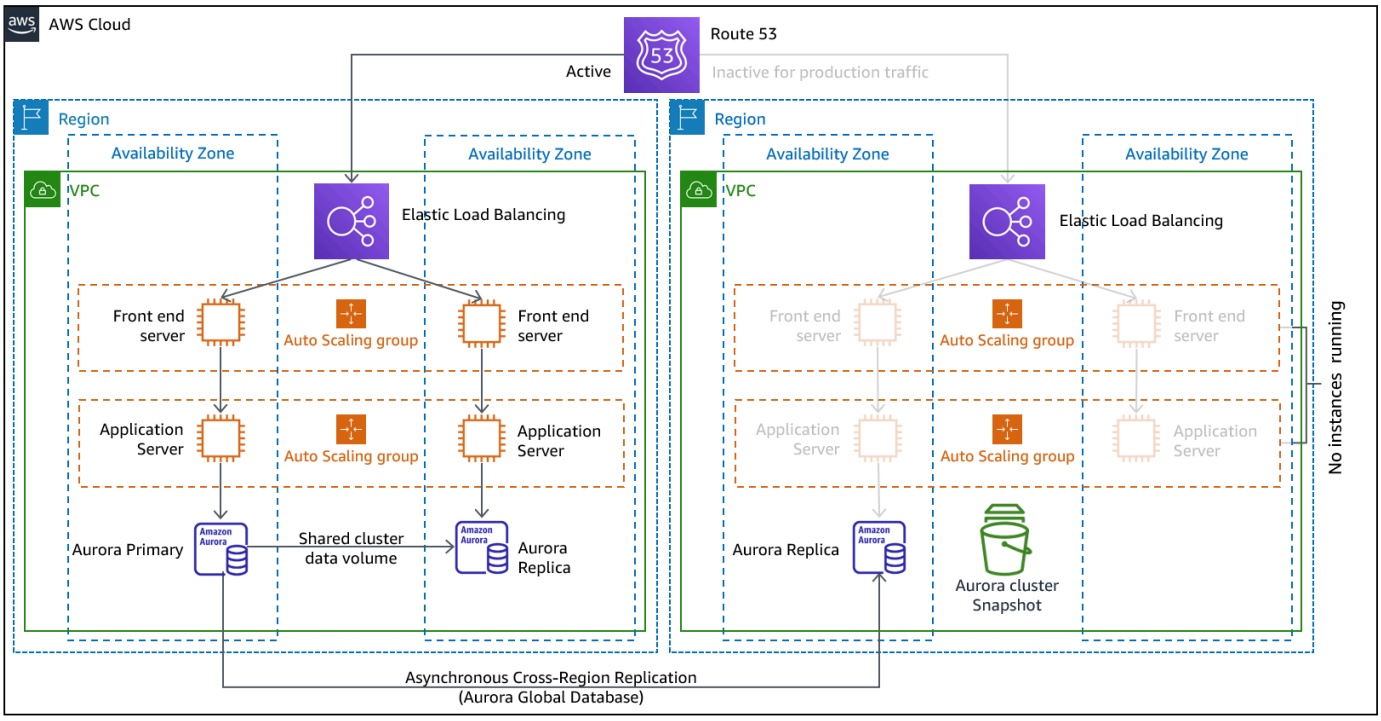

Abbildung 9: Architektur der Zündflamme

Ein Pilot-Light-Ansatz minimiert die laufenden Kosten für die Notfallwiederherstellung, indem die aktiven Ressourcen minimiert werden, und vereinfacht die Wiederherstellung im Notfall, da alle grundlegenden Infrastrukturanforderungen erfüllt sind. Bei dieser Wiederherstellungsoption

müssen Sie Ihren Bereitstellungsansatz ändern. Sie müssen in jeder Region Änderungen an der Kerninfrastruktur vornehmen und Änderungen an der Arbeitslast (Konfiguration, Code) gleichzeitig in jeder Region implementieren. Dieser Schritt kann vereinfacht werden, indem Sie Ihre Bereitstellungen automatisieren und Infrastructure as Code (IaC) verwenden, um die Infrastruktur über mehrere Konten und Regionen hinweg bereitzustellen (vollständige Infrastrukturbereitstellung in der primären Region und skalierte Infrastrukturbereitstellung herunterskaliert/abgeschaltete Infrastruktur in DR-Regionen). Es wird empfohlen, pro Region ein anderes Konto zu verwenden, um ein Höchstmaß an Ressourcen- und Sicherheitsisolierung zu gewährleisten (für den Fall, dass kompromittierte Anmeldeinformationen auch Teil Ihrer Notfallwiederherstellungspläne sind).

Mit diesem Ansatz müssen Sie sich auch gegen eine Datenkatastrophe wappnen. Kontinuierliche Datenreplikation schützt Sie vor einigen Arten von Notfällen, aber sie schützt Sie möglicherweise nicht vor Datenbeschädigung oder -vernichtung, sofern Ihre Strategie nicht auch die Versionierung von gespeicherten Daten oder Wiederherstellungsoptionen umfasst. point-in-time Sie können die replizierten Daten in der Notfallregion sichern, um point-in-time Backups in derselben Region zu erstellen.

AWS-Services

Neben der Nutzung der im Abschnitt Backup und Wiederherstellung beschriebenen AWS-Services zur Erstellung von point-in-time Backups sollten Sie auch die folgenden Services für Ihre Pilotstrategie in Betracht ziehen.

Für Pilot Light ist die kontinuierliche Datenreplikation auf Live-Datenbanken und Datenspeicher in der DR-Region der beste Ansatz für ein niedriges RPO (wenn sie zusätzlich zu den zuvor besprochenen point-in-time Backups verwendet wird). AWS bietet eine kontinuierliche, regionsübergreifende, asynchrone Datenreplikation für Daten mithilfe der folgenden Services und Ressourcen:

- Replikation mit Amazon Simple Storage Service (Amazon S3)
- Amazon RDS liest Repliken
- Globale Amazon Aurora Aurora-Datenbanken
- Globale Amazon DynamoDB-Tabellen
- Globale Amazon DocumentDB-Cluster
- Globaler Datenspeicher für Amazon ElastiCache (Redis OSS)

Dank kontinuierlicher Replikation sind Versionen Ihrer Daten in Ihrer DR-Region fast sofort verfügbar. Die tatsächlichen Replikationszeiten können mithilfe von Servicefunktionen wie S3 Replication Time

Control (S3 RTC) für S3-Objekte und Verwaltungsfunktionen der globalen Amazon Aurora Aurora-Datenbanken überwacht werden.

Wenn Sie einen Failover durchführen möchten, um Ihren read/write Workload von der Disaster Recovery-Region aus auszuführen, müssen Sie eine RDS-Read Replica zur primären Instance heraufstufen. Bei anderen DB-Instances als Aurora dauert der Vorgang einige Minuten, und der Neustart ist Teil des Prozesses. Für regionsübergreifende Replikation (CRR) und Failover mit RDS bietet die Verwendung der globalen Amazon Aurora Aurora-Datenbank mehrere Vorteile. Die globale Datenbank verwendet eine dedizierte Infrastruktur, sodass Ihre Datenbanken vollständig für Ihre Anwendung verfügbar sind. Sie kann in die sekundäre Region mit einer typischen Latenz von unter einer Sekunde repliziert werden (und innerhalb einer AWS-Region sind es deutlich weniger als 100 Millisekunden). Mit der globalen Amazon Aurora Aurora-Datenbank können Sie bei Leistungseinbußen oder -ausfällen in Ihrer primären Region eine der sekundären Regionen so befördern, dass sie in weniger als einer Minute Lese-/Schreibaufgaben übernimmt, selbst bei einem vollständigen regionalen Ausfall. Sie können Aurora auch so konfigurieren, dass die RPO-Verzögerungszeit aller sekundären Cluster überwacht wird, um sicherzustellen, dass mindestens ein sekundärer Cluster innerhalb Ihres Ziel-RPO-Fensters bleibt.

In Ihrer DR-Region muss eine verkleinerte Version Ihrer Kern-Workload-Infrastruktur mit weniger oder kleineren Ressourcen bereitgestellt werden. Mithilfe AWS CloudFormation können Sie Ihre Infrastruktur definieren und sie konsistent für alle AWS-Konten und AWS-Regionen bereitstellen. AWS CloudFormation verwendet vordefinierte Pseudo-Parameter, um das AWS-Konto und die AWS-Region zu identifizieren, in der es bereitgestellt wird. Daher können Sie Bedingungslogik in Ihren CloudFormation Vorlagen implementieren, um nur die verkleinerte Version Ihrer Infrastruktur in der DR-Region bereitzustellen. Bei EC2 Bereitstellungen liefert ein Amazon Machine Image (AMI) Informationen wie Hardwarekonfiguration und installierte Software. Sie können eine Image Builder Builder-Pipeline implementieren, die die AMIs benötigten Daten erstellt und diese sowohl in Ihre primäre als auch in Ihre Backup-Region kopiert. Auf diese Weise können Sie sicherstellen, dass diese AMIsGold-Tools über alles verfügen, was Sie benötigen, um Ihren Workload im Katastrophenfall in einer neuen Region neu bereitzustellen oder zu skalieren. EC2 Amazon-Instances werden in einer reduzierten Konfiguration bereitgestellt (weniger Instances als in Ihrer primären Region). Informationen zur Skalierung der Infrastruktur zur Unterstützung des Produktionsverkehrs finden Sie unter Amazon EC2 Auto Scaling im Abschnitt Warm Standby.

Bei einer active/passive Konfiguration wie einer Pilotlampe geht der gesamte Datenverkehr zunächst in die primäre Region und wechselt in die Notfallwiederherstellungsregion, wenn die primäre Region nicht mehr verfügbar ist. Dieser Failover-Vorgang kann entweder automatisch oder manuell eingeleitet werden. Automatisch eingeleitetes Failover auf der Grundlage von Zustandsprüfungen

oder Alarmen sollte mit Vorsicht verwendet werden. Selbst bei Anwendung der hier erörterten bewährten Methoden werden Wiederherstellungszeit und Wiederherstellungspunkt größer als Null sein, was zu einem gewissen Verlust an Verfügbarkeit und Daten führen kann. Wenn Sie einen Failover durchführen, obwohl dies nicht erforderlich ist (Fehlalarm), erleiden Sie diese Verluste. Daher wird häufig ein manuell initiierter Failover verwendet. In diesem Fall sollten Sie die Schritte für den Failover dennoch automatisieren, sodass die manuelle Auslösung wie ein Knopfdruck wirkt.

Bei der Nutzung von AWS Diensten sind mehrere Optionen für das Verkehrsmanagement zu berücksichtigen.

Eine Option ist die Verwendung von Amazon Route 53. Mit Amazon Route 53 können Sie mehrere IP-Endpunkte in einer oder mehreren AWS-Regionen mit einem Route 53-Domainnamen verknüpfen. Anschließend können Sie den Datenverkehr unter diesem Domainnamen an den entsprechenden Endpunkt weiterleiten. Beim Failover müssen Sie den Datenverkehr zum Wiederherstellungsendpunkt und vom primären Endpunkt weg verlagern. Amazon Route 53 Health Checks überwachen diese Endpunkte. Mithilfe dieser Zustandsprüfungen können Sie ein automatisch eingeleitetes DNS-Failover konfigurieren, um sicherzustellen, dass der Datenverkehr nur an fehlerfreie Endgeräte gesendet wird. Dies ist ein äußerst zuverlässiger Vorgang auf der Datenebene. Um dies mithilfe eines manuell initiierten Failovers zu implementieren, können Sie Amazon Application Recovery Controller (ARC) verwenden. Mit ARC können Sie Route 53-Zustandsprüfungen erstellen, die nicht wirklich den Zustand überprüfen, sondern stattdessen als Ein-/Ausschalter fungieren, über die Sie die volle Kontrolle haben. Mit der AWS-CLI oder dem AWS-SDK können Sie mithilfe dieser hochverfügbaren Datenebenen-API ein Failover-Skript erstellen. Ihr Skript schaltet diese Schalter (die Route 53-Zustandsprüfungen) um und weist Route 53 an, Datenverkehr an die Wiederherstellungsregion statt an die primäre Region zu senden. Eine weitere Option für manuell initiiertes Failover, die von einigen verwendet wurde, besteht darin, eine gewichtete Routing-Richtlinie zu verwenden und die Gewichtung der primären und der Wiederherstellungsregion so zu ändern, dass der gesamte Datenverkehr in die Wiederherstellungsregion geleitet wird. Beachten Sie jedoch, dass dies ein Vorgang auf Kontrollebene ist und daher nicht so robust ist wie der Datenebenenansatz mit Amazon Application Recovery Controller (ARC).

Eine weitere Option ist die Verwendung AWS Global Accelerator. Mithilfe von AnyCast IP können Sie mehrere Endpunkte in einer oder mehreren AWS-Regionen derselben statischen öffentlichen IP-Adresse oder Adressen zuordnen. AWS Global Accelerator leitet dann den Datenverkehr an den entsprechenden Endpunkt weiter, der dieser Adresse zugeordnet ist. Die Zustandsprüfungen von Global Accelerator überwachen die Endpunkte. Mithilfe dieser Integritätsprüfungen wird der Zustand Ihrer Anwendungen AWS Global Accelerator überprüft und der Benutzerverkehr automatisch an den fehlerfreien Anwendungsendpunkt weitergeleitet. Bei einem manuell eingeleiteten Failover können

Sie mithilfe von Verkehrswahlen einstellen, welcher Endpunkt Datenverkehr empfängt. Beachten Sie jedoch, dass es sich dabei um einen Vorgang auf der Kontrollebene handelt. Global Accelerator bietet geringere Latenzen für den Anwendungsendpunkt, da es das umfangreiche AWS-Edge-Netzwerk nutzt, um den Datenverkehr so schnell wie möglich auf den AWS-Netzwerk-Backbone zu übertragen. Global Accelerator vermeidet auch Caching-Probleme, die bei DNS-Systemen (wie Route 53) auftreten können.

Amazon CloudFront bietet Origin-Failover an, bei dem, wenn eine bestimmte Anfrage an den primären Endpunkt fehlschlägt, die CloudFront Anfrage an den sekundären Endpunkt weitergeleitet wird. Im Gegensatz zu den zuvor beschriebenen Failover-Vorgängen werden alle nachfolgenden Anfragen immer noch an den primären Endpunkt weitergeleitet, und das Failover wird für jede Anfrage durchgeführt.

AWS Elastische Notfallwiederherstellung

AWS Elastic Disaster Recovery (DRS) repliziert kontinuierlich servergehostete Anwendungen und servergehostete Datenbanken aus beliebigen Quellen und AWS verwendet dabei die Replikation des zugrunde liegenden Servers auf Blockebene. Elastic Disaster Recovery ermöglicht es Ihnen, eine Region AWS Cloud als Disaster Recovery-Ziel für einen Workload, der vor Ort oder bei einem anderen Cloud-Anbieter gehostet wird, und dessen Umgebung zu verwenden. Es kann auch für die Notfallwiederherstellung von AWS gehosteten Workloads verwendet werden, wenn diese nur aus Anwendungen und Datenbanken bestehen, auf denen gehostet wird EC2 (d. h. nicht auf RDS). Elastic Disaster Recovery verwendet die Pilot Light-Strategie, bei der eine Kopie von Daten und „ausgeschalteten“ Ressourcen in einer Amazon Virtual Private Cloud (Amazon VPC) verwaltet wird, die als Staging-Bereich genutzt wird. Wenn ein Failover-Ereignis ausgelöst wird, werden die bereitgestellten Ressourcen verwendet, um automatisch eine Bereitstellung mit voller Kapazität in der Amazon-Ziel-VPC zu erstellen, die als Wiederherstellungsstandort verwendet wird.

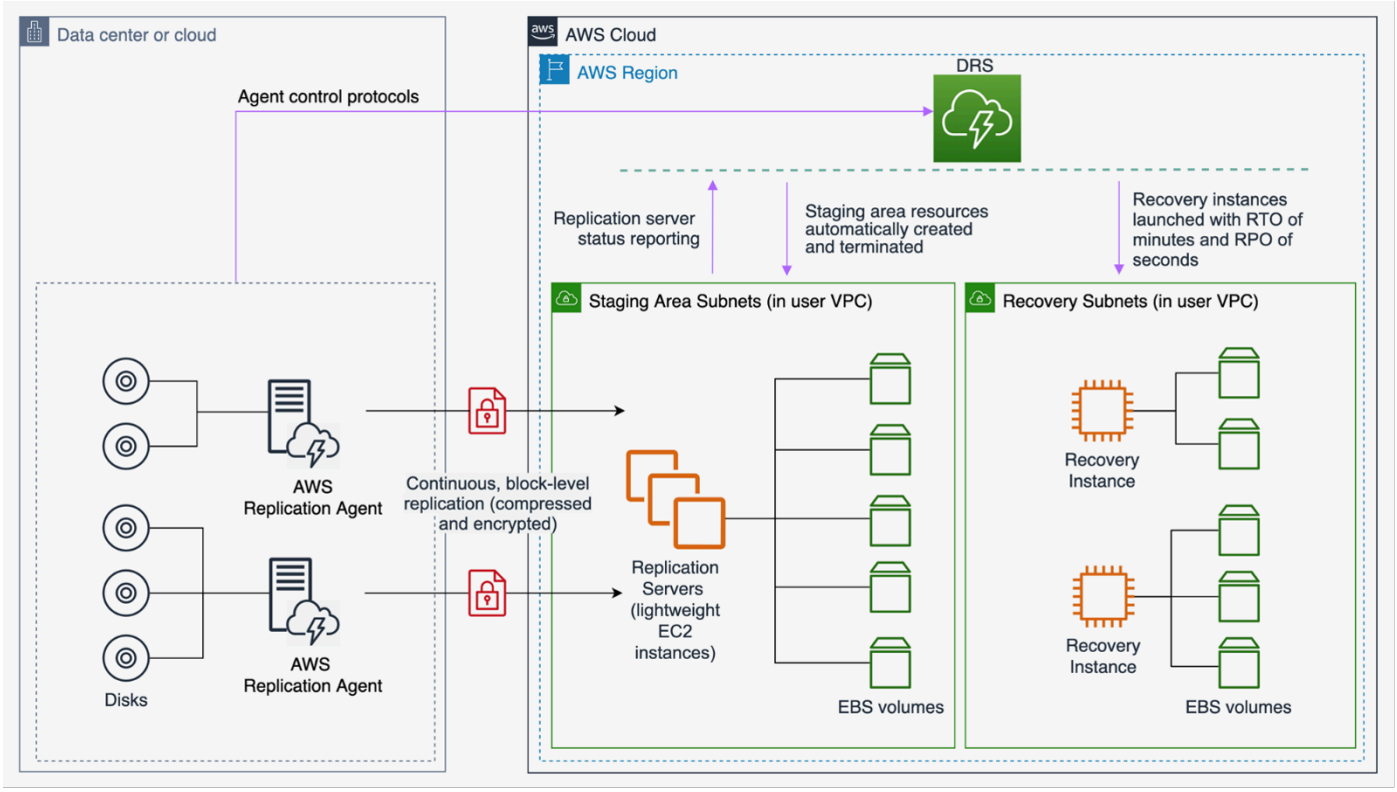

Abbildung 10: AWS Elastic Disaster Recovery-Architektur

Warmer Bereitschaftsmodus

Beim Warm-Standby-Ansatz wird sichergestellt, dass eine herunterskalierte, aber voll funktionsfähige Kopie Ihrer Produktionsumgebung in einer anderen Region vorhanden ist. Dieser Ansatz erweitert das Konzept des Pilot Light und verkürzt die Zeit bis zur Wiederherstellung, da die Workload in einer anderen Region ständig präsent ist. Dieser Ansatz ermöglicht es Ihnen auch, Tests einfacher durchzuführen oder kontinuierliche Tests zu implementieren, um das Vertrauen in Ihre Fähigkeit zu stärken, sich nach einem Notfall wieder zu erholen.

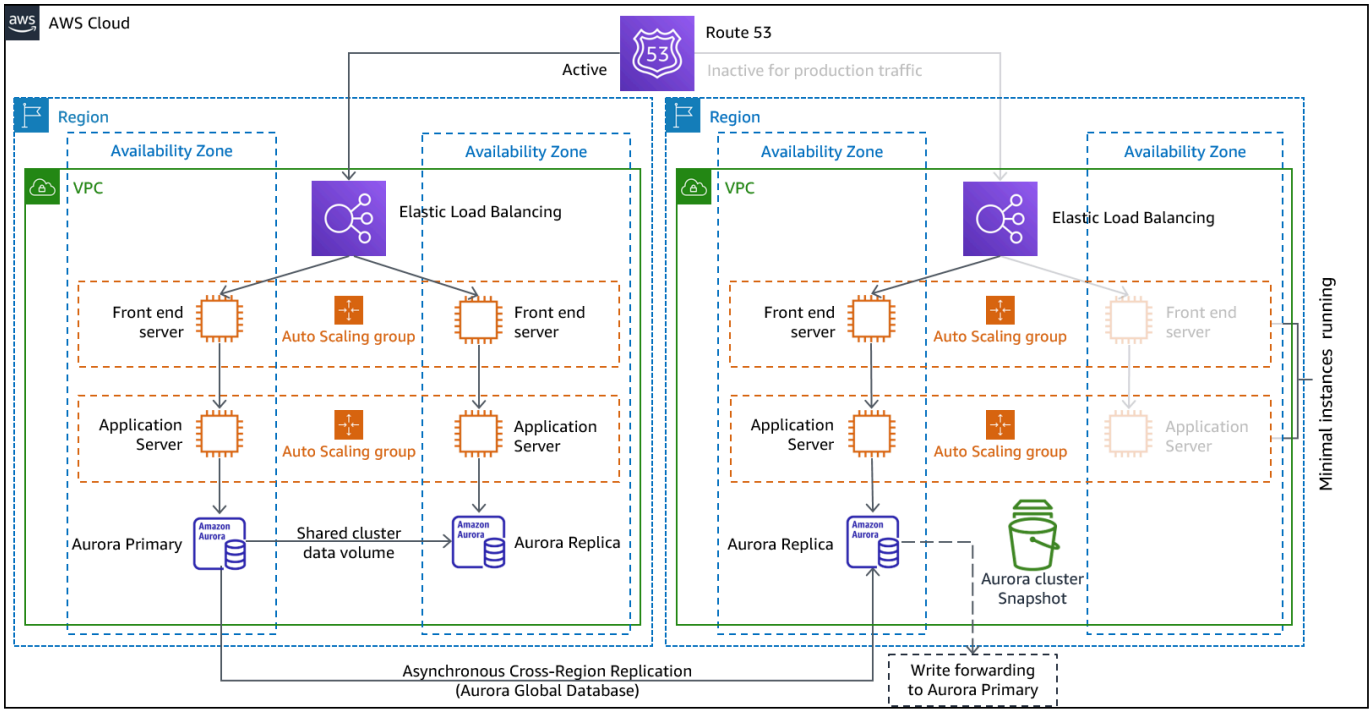

Abbildung 11: Warm-Standby-Architektur

Hinweis: Der Unterschied zwischen Pilotlicht und Warm-Standby kann manchmal schwer zu verstehen sein. Beide beinhalten eine Umgebung in Ihrer DR-Region mit Kopien der Ressourcen Ihrer primären Region. Der Unterschied besteht darin, dass die Kontrolllampe Anfragen nicht bearbeiten kann, ohne dass zuvor zusätzliche Maßnahmen ergriffen werden, wohingegen der Warm-Standby-Modus den Verkehr (bei reduzierter Kapazität) sofort abwickeln kann. Beim Pilot-Light-Ansatz müssen Sie Server „einschalten“, eventuell zusätzliche (nicht zum Kerngeschäft gehörende) Infrastruktur bereitstellen und hochskalieren, wohingegen bei Warm-Standby lediglich eine Skalierung erforderlich ist (alles ist bereits implementiert und läuft). Verwenden Sie Ihre RTO- und RPO-Anforderungen, um sich zwischen diesen Ansätzen zu entscheiden.

AWS-Services

Alle AWS-Services, die unter Backup and Restore und Pilot Light fallen, werden auch im Warm-Standby für Datensicherung, Datenreplikation, active/passive Datenweiterleitung und Bereitstellung der Infrastruktur einschließlich EC2 Instances verwendet.

Amazon EC2 Auto Scaling wird verwendet, um Ressourcen wie EC2 Amazon-Instances, Amazon ECS-Aufgaben, Amazon DynamoDB-Durchsatz und Amazon Aurora Aurora-Repliken innerhalb einer AWS-Region zu skalieren. Amazon EC2 Auto Scaling skaliert die Bereitstellung von EC2

Instances über Availability Zones innerhalb einer AWS-Region und sorgt so für Stabilität innerhalb dieser Region. Verwenden Sie Auto Scaling, um Ihre DR-Region im Rahmen einer Pilotphase- oder Warm-Standby-Strategie auf die volle Produktionskapazität hochzuskalieren. Erhöhen Sie EC2 beispielsweise die gewünschte Kapazitätseinstellung in der Auto Scaling Scaling-Gruppe. Sie können diese Einstellung manuell über das AWS Management Console, automatisch über das AWS-SDK oder durch erneutes Bereitstellen Ihrer AWS CloudFormation Vorlage mit dem neuen gewünschten Kapazitätswert anpassen. Sie können AWS CloudFormation Parameter verwenden, um die erneute Bereitstellung der CloudFormation Vorlage zu vereinfachen. Stellen Sie sicher, dass die Servicekontingenten in Ihrer DR-Region hoch genug festgelegt sind, um Sie nicht daran zu hindern, die Produktionskapazität zu erhöhen.

Da es sich bei Auto Scaling um eine Aktivität auf der Kontrollebene handelt, verringert die Abhängigkeit davon die Widerstandsfähigkeit Ihrer gesamten Wiederherstellungsstrategie. Es ist ein Kompromiss. Sie können sich dafür entscheiden, ausreichend Kapazität bereitzustellen, sodass die Wiederherstellungsregion die gesamte Produktionslast wie bereitgestellt bewältigen kann. Diese statisch stabile Konfiguration wird als Hot-Standby bezeichnet (siehe nächster Abschnitt). Oder Sie können sich dafür entscheiden, weniger Ressourcen bereitzustellen, was weniger kostet, aber auf Auto Scaling angewiesen ist. Bei einigen DR-Implementierungen werden genügend Ressourcen bereitgestellt, um den anfänglichen Verkehr zu bewältigen, wodurch ein niedriges RTO gewährleistet wird, und sich dann auf Auto Scaling verlassen, um den nachfolgenden Verkehr hochzufahren.

Multi-Site Aktiv/Aktiv

Im Rahmen einer Aktiv/Passiv-Strategie für mehrere Standorte können Sie Ihren Workload gleichzeitig in mehreren Regionen ausführen. An mehreren Standorten active/active wird Datenverkehr aus allen Regionen, in denen sie bereitgestellt wird, bedient, wohingegen Hot-Standby nur Datenverkehr aus einer einzigen Region verarbeitet und die anderen Regionen nur für die Notfallwiederherstellung verwendet werden. Bei einem standortübergreifenden active/active Ansatz können Benutzer auf Ihre Workloads in allen Regionen zugreifen, in denen sie bereitgestellt werden. Dieser Ansatz ist der komplexeste und teuerste Ansatz für die Notfallwiederherstellung, aber er kann die Wiederherstellungszeit bei den meisten Katastrophen auf nahezu Null reduzieren, wenn die richtige Technologie gewählt und implementiert wird (Datenbeschädigung kann jedoch auf Backups angewiesen sein, was in der Regel dazu führt, dass ein Wiederherstellungspunkt ungleich Null ist). Hot-Standby verwendet eine active/passive Konfiguration, bei der Benutzer nur an eine einzige Region weitergeleitet werden und DR-Regionen keinen Datenverkehr aufnehmen. Die meisten Kunden sind der Meinung, dass es sinnvoll ist, sie aktiv/aktiv zu verwenden, wenn sie eine vollständige Umgebung in der zweiten Region einrichten möchten. Wenn Sie nicht beide Regionen

für die Verwaltung des Benutzerverkehrs verwenden möchten, bietet Warm Standby alternativ einen wirtschaftlicheren und betrieblich weniger komplexen Ansatz.

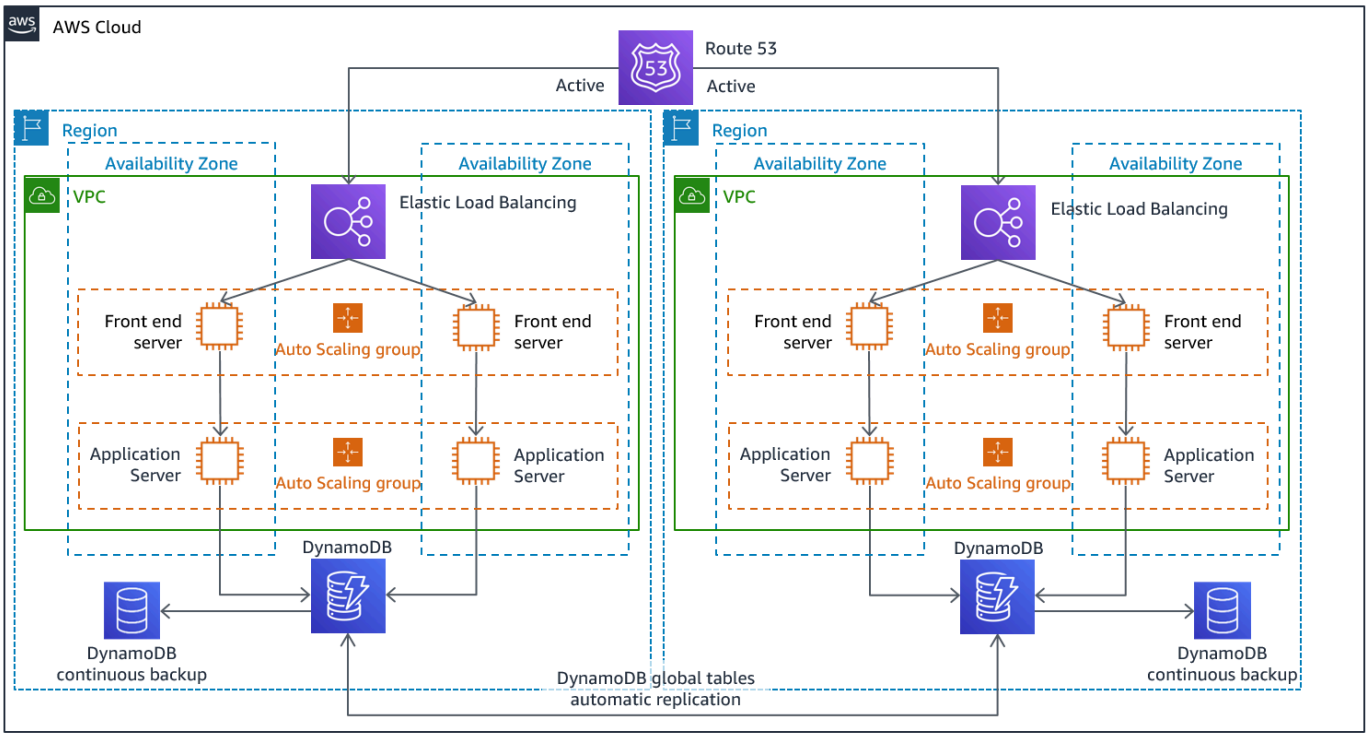

Abbildung 12: active/active Architektur mit mehreren Standorten (ändern Sie einen aktiven Pfad in Inaktiv für Hot-Standby)

Da ein Ansatz mit mehreren active/active, because the workload is running in more than one Region, there is no such thing as failover in this scenario. Disaster recovery testing in this case would focus on how the workload reacts to loss of a Region: Is traffic routed away from the failed Region? Can the other Region(s) handle all the traffic? Testing for a data disaster is also required. Backup and recovery are still required and should be tested regularly. It should also be noted that recovery times for a data disaster involving data corruption, deletion, or obfuscation will always be greater than zero and the recovery point will always be at some point before the disaster was discovered. If the additional complexity and cost of a multi-site active/active Standorten (oder Hot-Standby) erforderlich ist, um Wiederherstellungszeiten von nahezu Null einzuhalten, sollten zusätzliche Anstrengungen unternommen werden, um die Sicherheit aufrechtzuerhalten und menschliches Versagen zu verhindern, um menschliche Katastrophen zu vermeiden.

AWS-Services

Alle AWS-Services, die unter Backup and Restore, Pilot Light und Warm Standby fallen, werden hier auch für point-in-time Datensicherung, Datenreplikation, active/active Datenweiterleitung sowie Bereitstellung und Skalierung der Infrastruktur einschließlich EC2 Instances verwendet.

Für die zuvor erörterten active/passive Szenarien (Pilot Light und Warm Standby) AWS Global Accelerator können sowohl Amazon Route 53 als auch für die Weiterleitung des Netzwerkverkehrs in die aktive Region verwendet werden. Für die hier active/active vorgestellte Strategie ermöglichen beide Dienste auch die Definition von Richtlinien, mit denen festgelegt wird, welche Benutzer zu welchem aktiven regionalen Endpunkt gehen. Außerdem stellen AWS Global Accelerator Sie eine Verkehrswahl ein, um den Prozentsatz des Datenverkehrs zu steuern, der an jeden Anwendungsendpunkt geleitet wird. Amazon Route 53 unterstützt diesen prozentualen Ansatz sowie mehrere andere verfügbare Richtlinien, einschließlich Richtlinien, die auf Geonähe und Latenz basieren. Global Accelerator nutzt automatisch das umfangreiche Netzwerk von AWS-Edge-Servern, um den Datenverkehr so schnell wie möglich in den AWS-Netzwerk-Backbone einzubinden, was zu geringeren Latenzen bei Anfragen führt.

Die asynchrone Datenreplikation mit dieser Strategie ermöglicht einen RPO-Wert von nahezu Null. AWS-Services wie Amazon Aurora Global Database verwenden eine spezielle Infrastruktur, sodass Ihre Datenbanken vollständig für Ihre Anwendung verfügbar sind und in bis zu fünf sekundäre Regionen mit einer typischen Latenz von unter einer Sekunde repliziert werden können. With active/passive strategies, writes occur only to the primary Region. The difference with active/active entwirft, wie die Datenkonsistenz bei Schreibvorgängen in jede aktive Region gehandhabt wird. Es ist üblich, Lesevorgänge für Benutzer so zu gestalten, dass sie von der Region aus zugestellt werden, die ihnen am nächsten ist. Dies wird als lokale Lesevorgänge bezeichnet. Bei Schreibvorgängen stehen Ihnen mehrere Optionen zur Verfügung:

- Bei einer globalen Schreibstrategie werden alle Schreibvorgänge an eine einzige Region weitergeleitet. Falls diese Region ausfällt, wird eine andere Region befördert, sodass sie Schreibvorgänge akzeptiert. Die globale Aurora-Datenbank eignet sich hervorragend für Write Global, da sie die regionsübergreifende Synchronisation mit Lesereplikaten unterstützt und Sie eine der sekundären Regionen in weniger als einer Minute zur Übernahme von read/write Aufgaben ernennen können. Aurora unterstützt auch die Schreibweiterleitung, sodass sekundäre Cluster in einer globalen Aurora-Datenbank SQL-Anweisungen, die Schreibvorgänge ausführen, an den primären Cluster weiterleiten können.
- Eine lokale Schreibstrategie leitet Schreibvorgänge in die nächstgelegene Region weiter (genau wie Lesevorgänge). Die globalen Tabellen von Amazon DynamoDB ermöglichen eine solche

Strategie und ermöglichen Lese- und Schreibvorgänge aus jeder Region, in der Ihre globale Tabelle bereitgestellt wird. Globale Amazon DynamoDB-Tabellen verwenden einen Last-Writer-Wins-Abgleich zwischen gleichzeitigen Aktualisierungen.

- Bei einer partitionierten Schreibstrategie werden Schreibvorgänge anhand eines Partitionsschlüssels (wie einer Benutzer-ID) einer bestimmten Region zugewiesen, um Schreibkonflikte zu vermeiden. Die bidirektional konfigurierte Amazon S3 S3-Replikation kann für diesen Fall verwendet werden und unterstützt derzeit die Replikation zwischen zwei Regionen. Achten Sie bei der Implementierung dieses Ansatzes darauf, die Synchronisierung von Replikatänderungen für beide Buckets A und B zu aktivieren, um Änderungen an Replikat-Metadaten wie Objektzugriffskontrolllisten (ACLs), Objekt-Tags oder Objektsperren für die replizierten Objekte zu replizieren. Sie können auch konfigurieren, ob Löschmarkierungen zwischen Buckets in Ihren aktiven Regionen repliziert werden sollen oder nicht. Neben der Replikation muss Ihre Strategie auch point-in-time Backups zum Schutz vor Datenbeschädigung oder -vernichtung beinhalten.

AWS CloudFormation ist ein leistungsstarkes Tool zur Durchsetzung einer konsistent bereitgestellten Infrastruktur zwischen AWS-Konten in mehreren AWS-Regionen. AWS CloudFormation StackSetserweitert diese Funktionalität, indem es Ihnen ermöglicht, CloudFormation Stacks für mehrere Konten und Regionen mit einem einzigen Vorgang zu erstellen, zu aktualisieren oder zu löschen. AWS CloudFormation Verwendet zwar YAML oder JSON, um Infrastruktur als Code zu definieren, AWS Cloud Development Kit (AWS CDK)ermöglicht es Ihnen jedoch, Infrastruktur als Code mithilfe vertrauter Programmiersprachen zu definieren. Ihr Code wird konvertiert CloudFormation , der dann zur Bereitstellung von Ressourcen in AWS verwendet wird.

Erkennung

Es ist wichtig, so schnell wie möglich zu wissen, dass Ihre Workloads nicht die Geschäftsergebnisse liefern, die sie erzielen sollten. Auf diese Weise können Sie schnell einen Notfall ausrufen und sich nach einem Vorfall erholen. Bei aggressiven Wiederherstellungszielen ist diese Reaktionszeit in Verbindung mit entsprechenden Informationen entscheidend, um die Wiederherstellungsziele zu erreichen. Wenn Ihr Ziel für die Wiederherstellung eine Stunde ist, müssen Sie den Vorfall erkennen, das entsprechende Personal benachrichtigen, Ihre Eskalationsprozesse einleiten, Informationen (falls vorhanden) zur voraussichtlichen Wiederherstellungszeit auswerten (ohne den DR-Plan auszuführen), einen Notfall ausrufen und innerhalb einer Stunde wiederherstellen.

> **Note**
>
> Wenn die Beteiligten beschließen, DR nicht in Anspruch zu nehmen, obwohl das RTO gefährdet wäre, sollten die DR-Pläne und -Ziele neu bewertet werden. Die Entscheidung, DR-Pläne nicht in Anspruch zu nehmen, kann darauf zurückzuführen sein, dass die Pläne unzureichend sind oder dass es an Vertrauen in die Ausführung mangelt.

Es ist wichtig, die Erkennung, Benachrichtigung, Eskalation, Entdeckung und Erklärung von Vorfällen in Ihre Planung und Zielsetzung einzubeziehen, um realistische, erreichbare Ziele zu erreichen, die einen geschäftlichen Nutzen bieten.

AWS veröffentlicht unsere meisten up-to-the-minute Informationen zur Serviceverfügbarkeit auf dem Service Health Dashboard. Schauen Sie jederzeit vorbei, um aktuelle Statusinformationen zu erhalten, oder abonnieren Sie einen RSS-Feed, um über Unterbrechungen bei jedem einzelnen Service informiert zu werden. Wenn Sie in Echtzeit ein Betriebsproblem mit einem unserer Dienste haben, das nicht im Service Health Dashboard angezeigt wird, können Sie eine Support-Anfrage stellen.

Das AWS Health Dashboardenthält Informationen zu AWS Health Ereignissen, die sich auf Ihr Konto auswirken können. Diese Informationen werden auf zweierlei Weise bereitgestellt: in einem Dashboard, in dem aktuelle und anstehende Ereignisse sortiert nach Kategorie angezeigt werden, und in einem vollständigen Protokoll, in dem alle Ereignisse der letzten 90 Tage angezeigt werden.

Für die strengsten RTO-Anforderungen können Sie automatisiertes Failover auf der Grundlage von Integritätsprüfungen implementieren. Entwerfen Sie Integritätsprüfungen, die für die

Benutzererfahrung repräsentativ sind und auf wichtigen Leistungsindikatoren basieren. Bei gründlichen Zustandsprüfungen werden wichtige Funktionen Ihres Workloads berücksichtigt und gehen über oberflächliche Heartbeat-Checks hinaus. Verwenden Sie tiefgreifende Gesundheitschecks, die auf mehreren Signalen basieren. Gehen Sie bei diesem Ansatz vorsichtig vor, damit Sie keine Fehlalarme auslösen, da ein Failover, wenn dies nicht erforderlich ist, an sich schon Verfügbarkeitsrisiken mit sich bringen kann.

Testen der Notfallwiederherstellung

Testen Sie die Disaster Recovery-Implementierung, um die Implementierung zu validieren, und testen Sie regelmäßig den Failover zur DR-Region Ihres Workloads, um sicherzustellen, dass RTO und RPO eingehalten werden.

Ein Muster, das es zu vermeiden gilt, ist die Entwicklung von Wiederherstellungspfaden, die selten ausgeführt werden. So könnten Sie beispielsweise einen zweiten Datenspeicher unterhalten, der nur für Leseabfragen verwendet wird. Wenn Sie Daten in einen Datenspeicher schreiben und der primäre Datenspeicher einen Fehler ausgibt, können Sie einen Failover auf den zweiten Datenspeicher durchführen. Wenn Sie diesen Failover nicht regelmäßig testen, werden Sie möglicherweise feststellen, dass Ihre Annahmen zu den Möglichkeiten des sekundären Datenspeichers unzutreffend sind. Die Kapazität der sekundären Region, die beim letzten Test möglicherweise ausreichend war, kann die Last in diesem Szenario möglicherweise nicht mehr aushalten, oder die Servicekontingenten in der sekundären Region sind möglicherweise nicht ausreichend.

Unsere Erfahrungen haben gezeigt, dass bei einer Wiederherstellung nach einem Fehler nur der Pfad funktioniert, den Sie regelmäßig testen. Aus diesem Grund ist es am besten, über eine geringe Anzahl von Wiederherstellungspfaden zu verfügen.

Sie können Wiederherstellungsmuster erstellen und diese regelmäßig testen. Wenn Sie über einen komplexen oder kritischen Wiederherstellungspfad verfügen, müssen Sie diesen Fehler dennoch regelmäßig in der Produktion ausführen, um zu überprüfen, ob der Wiederherstellungspfad funktioniert.

Managen Sie Konfigurationsabweichungen in der DR-Region. Stellen Sie sicher, dass Ihre Infrastruktur, Daten und Konfiguration in der DR-Region den Anforderungen entsprechen. Überprüfen Sie beispielsweise, ob AMIs und die Servicequotas zutreffen up-to-date.

Sie können Ihre AWS ConfigAWS-Ressourcenkonfigurationen kontinuierlich überwachen und aufzeichnen. AWS Config kann Drift erkennen und AWS Systems Manager Automation auslösen, um Drift zu beheben und Alarme auszulösen. AWS CloudFormationkann außerdem Abweichungen in Stacks erkennen, die Sie installiert haben.

Schlussfolgerung

Kunden sind für die Verfügbarkeit ihrer Anwendungen in der Cloud verantwortlich. Es ist wichtig, zu definieren, was ein Notfall ist, und einen Notfallwiederherstellungsplan zu haben, der diese Definition und die möglichen Auswirkungen auf die Geschäftsergebnisse widerspiegelt. Erstellen Sie auf der Grundlage von Folgenanalysen und Risikobewertungen ein Recovery Time Objective (RTO) und ein Recovery Point Objective (RPO) und wählen Sie dann die geeignete Architektur zur Abwehr von Katastrophen aus. Stellen Sie sicher, dass Katastrophen rechtzeitig erkannt werden können — es ist wichtig zu wissen, wann die Ziele gefährdet sind. Stellen Sie sicher, dass Sie über einen Plan verfügen, und validieren Sie ihn mit Tests. Disaster-Recovery-Pläne, die nicht validiert wurden, laufen Gefahr, dass sie aufgrund mangelnden Vertrauens oder aufgrund der Nichterfüllung der Disaster-Recovery-Ziele nicht umgesetzt werden.

Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Alex Livingstone, Praxisleiter Cloud-Betrieb, AWS Enterprise Support
- Seth Eliot, leitender Architekt für Zuverlässigkeitslösungen, Amazon Web Services

Weitere Informationen

Weitere Informationen finden Sie unter:

- AWS Zentrum für Architektur
- Säule der Zuverlässigkeit, AWS Well-Architected Framework
- Checkliste für den Notfallwiederherstellungsplan
- Durchführung von Gesundheitschecks
- Disaster Recovery (DR) -Architektur auf AWS, Teil I: Strategien für die Wiederherstellung in der Cloud
- Disaster Recovery (DR) -Architektur auf AWS, Teil II: Backup und Wiederherstellung mit Rapid Recovery
- Disaster Recovery (DR) -Architektur auf AWS, Teil III: Pilot Light und Warm Standby
- Disaster Recovery (DR) -Architektur auf AWS, Teil IV: Aktiv/Aktiv an mehreren Standorten
- Erstellen von Mechanismen für die Notfallwiederherstellung mit Amazon Route 53
- Minimierung der Abhängigkeiten bei der Planung der Notfallwiederherstellung
- Praktische, AWS Well-Architected Recovery-Labore
- AWS Lösungsimplementierungen: Multi-Region Application Architecture
- AWS re:Invent 2018: Architekturmuster für aktiv-aktive Anwendungen mit mehreren Regionen (09-R2) ARC2

Dokumentverlauf

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Änderung	Beschreibung	Datum
Kleinere Updates	Durchweg Bugfixes und zahlreiche kleinere Änderungen.	1. April 2022
Whitepaper aktualisiert	Kleinere redaktionelle Aktualisierungen.	21. März 2022
Whitepaper aktualisiert	Es wurden Informationen zur Datenebene und zur Steuerebene hinzugefügt. Es wurden weitere Details zur Implementierung von active/passive Failover hinzugefügt. CloudEndure Disaster Recovery wurde durch AWS Elastic Disaster Recovery ersetzt.	17. Februar 2022
Kleines Update	AWS Well-Architected Tool Informationen wurden hinzugefügt.	11. Februar 2022
Erste Veröffentlichung	Whitepaper zuerst veröffentlicht.	12. Februar 2021

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS-Produktangebote und -praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS-Produkte oder -Services werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, nicht zu den Vereinbarung von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.