aws

개발자 가이드

Amazon Route 53 애플리케이션 복구 컨트롤러

Amazon Route 53 애플리케이션 복구 컨트롤러: 개발자 가이드

Table of Contents

Amazon Route 53 Application Recovery Controller란 무엇입니까?

Amazon Route 53 애플리케이션 복구 컨트롤러 (Route 53 ARC) 를 사용하면 실행 중인 애플리케이션을 더 빠르게 복구할 수 있도록 준비하고 완료할 수 AWS있습니다. Route 53 ARC는 두 가지 기능 세트를 제공합니다. 하나는 영역 이동 및 영역 자동 이동을 포함하는 다중 가용 영역 (AZ) 복구이고 다른 하나는 라우팅 제어 및 준비 상태 확인을 포함하는 다중 지역 복구입니다. Route 53 ARC를 사용하면 가용성이 높은 복구 도구를 활용하여 다중 지역 또는 다중 AZ 애플리케이션에 영향을 미치는 장애를 신속하게 완화할 수 있습니다. 또한 준비 상태 검사를 사용하여 애플리케이션과 리소스가 복구 준비가 되었는지 여부에 대한 통찰력을 얻을 수 있습니다.

AWS 글로벌 클라우드 인프라는 내결함성과 복원력을 제공하며, 각 가용 영역은 완전히 격리된 여러 가용 영역으로 AWS 리전 구성되어 있습니다. Route 53 ARC는 이 AWS 구조 내에서 작동하여 애플리케이션의 복원력을 높이는 데 도움이 됩니다.

다중 AZ 복구

에서 AWS가용 영역을 활용하도록 구축된 애플리케이션이 있는 경우 영역 이동을 사용하여 AZ 장애를 신속하게 격리하고 복구할 수 있습니다. 영역 전환을 통해 지원되는 리소스의 트래픽을 AZ에서 다른 AZ로 일시적으로 이동하여 가용 영역 (AZ) 장애로부터 복구할 수 있습니다. AWS 리전영역 전환을 시작하면 예를 들어 개발자의 잘못된 코드 배포나 단일 가용 영역의 AWS 장애 등으로부터 애플리케이션을 빠르게 복구할 수 있습니다. 트래픽을 다른 곳으로 이동하면 한 AZ에 문제가 발생했을 때 애플리케이션을 사용하는 클라이언트에 미치는 영향을 줄일 수 있습니다.

한 지역의 계정에서 지원되는 모든 리소스에 대해 영역 전환을 시작할 수 있습니다. AWS 서비스는 Route 53 ARC에서 영역 이동을 통해 지원되는 AWS 리소스를 자동으로 등록하므로 언제든지 영역 이동을 시작할 수 있습니다.

영역 자동 전환은 Route 53 ARC의 기능으로, 지원되는 리소스의 트래픽을 AZ에서 다른 AZ로 대신 해당 지역의 정상 AZ로 AWS 이동하도록 승인할 수 있습니다. AWS 리전 AWS 내부 원격 측정 결과 한 지역의 AZ에 잠재적으로 고객에게 영향을 미칠 수 있는 장애가 있는 것으로 확인되면 자동 전환을 시작합니다. 내부 텔레메트리는 AWS 네트워크, Amazon EC2 및 Elastic Load Balancing 서비스를 비롯한 여러 소스의 메트릭을 통합합니다.

영역 이동 및 자동 이동은 일시적입니다. 수동 구역 이동을 시작할 때는 (연장 가능한) 만료를 처음에는 최대 3일로 지정해야 합니다. 계속해서 트래픽이 AZ에 들어가지 않도록 하려면 영역 이동을 업데이트하고 새 만료를 설정할 수 있습니다. 영역 자동 이동을 사용하면 지표에 더 이상 문제나 잠재적 문제가 없다고 표시되면 자동 이동이 AWS 종료됩니다.

이러한 기능에 대해 자세히 알아보려면 다음 장을 참조하십시오.

- Amazon Route 53 Application Recovery Controller의 영역 전환
- Amazon Route 53 Application Recovery Controller의 영역 자동 전환

다중 리전 복구

작업을 계속하기 위해 다른 AWS 리전 응용 프로그램에서 작동하도록 설계한 응용 프로그램이 있는 경우 라우팅 제어를 사용하여 장애 조치를 수행할 수 있습니다. 라우팅 제어를 사용하면 문제가 발생했을 때 다른 트래픽으로 트래픽을 페일오버할 수 있으므로 애플리케이션의 가용성을 유지할 수 있습니다. AWS 리전 라우팅 제어에는 사용자가 정의한 가드레일을 적용하여 의도하지 않은 결과를 방지하는 데 도움이 되는 안전 규칙이 포함됩니다. 이러한 규칙을 사용하면 예를 들어 활성 또는 대기 상태의 애플리케이션 복제본 중 하나만 한 번에 활성화되어 사용 중인지 확인할 수 있습니다.

다중 지역 복구의 경우 Route 53 ARC를 사용하면 DNS 트래픽을 AWS 리전페일오버할 수 있습니다. Route 53 ARC의 매우 안정적인 라우팅 제어를 사용하면 장애가 있는 지역에서 정상 지역으로 트래픽을 다시 라우팅하여 애플리케이션을 복구할 수 있습니다.

준비 상태 확인을 통해 Route 53 ARC는 AWS 리소스 할당량, 용량 및 네트워크 라우팅 정책을 지속적으로 모니터링하고 복제본으로의 장애 조치 및 복구 기능에 영향을 미칠 수 있는 변경 사항을 알려줄 수 있습니다. 지속적인 준비 상태 검사를 통해 다중 지역 애플리케이션을 장애 조치 트래픽을 처리하도록 확장 및 구성된 상태로 지속적으로 유지할 수 있습니다. 준비 확인은 Route 53 ARC를 처음 구성할 때와 정상적인 애플리케이션 작동 중에 유용합니다. 준비 상태 검사는 이벤트 중 페일오버를 위한 중요 경로에서 사용하기 위한 것이 아닙니다.

이러한 기능에 대한 자세한 내용은 다음 장을 참조하십시오.

- Amazon Route 53 Application Recovery Controller의 라우팅 제어
- Amazon Route 53 Application Recovery Controller의 준비 확인

Amazon Route 53 애플리케이션 복구 컨트롤러의 다중 AZ 및 다중 지역 복구 기능 비교

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동, 영역 자동 이동 및 라우팅 제어는 모두 빠른 복구를 달성하고 애플리케이션의 복원력을 보장하는 데 도움이 됩니다. AWS 이러한 옵션은 가용성이 높으며 애플리케이션의 지연 시간이 증가하거나 가용성이 저하되는 시나리오에서 복구를 지원하는 데 도움이 됩니다. 이러한 옵션을 사용하면 트래픽을 고립된 장애로부터 멀리 이동시켜 장애로 인한 영향과 시간 손실을 제한함으로써 애플리케이션을 신속하게 복구할 수 있습니다.

라우팅 제어는 주로 여러 지역 (다중 지역) 에 있는 AWS 애플리케이션에 중점을 두는 반면, AWS 영역 이동 및 영역 자동 이동은 다중 AZ 애플리케이션을 사용하는 로드 밸런서의 트래픽 이동만 지원합니다. 이 섹션의 설명처럼 다른 차이점도 있습니다.

다음 표의 정보에는 영역 이동, 영역 자동 이동, 라우팅 제어의 주요 기능 중 일부와 각 옵션의 비교 내용이 포함되어 있습니다. 이러한 설명을 통해 특정 옵션이 조직의 재해 복구 요구 사항에 가장 적합할 수 있는 방법을 더 잘 이해할 수 있습니다.

라우팅 제어	영역 전환	영역 자동 전환
리전 트래픽을 한 AWS 지역에서 다른 지역으로 다시 라우팅합니다 (주로). 가용 영역 간 재라우팅에도 사용 가능	영역 트래픽을 가용 영역에서 멀리 이동 트래픽은 특정 대상이 아닌 리전 내 다른 가용 영역으로 이동	영역 트래픽을 가용 영역에서 멀리 이동 트래픽은 특정 대상이 아닌 리전 내 다른 가용 영역으로 이동
설정 필요 구성 및 설정 필요	설정 없이 사용 가능 지원되는 서비스에서 자동으로 활성화됨 (현재 Network Load Balancer 및 Application Load Balancer)	연습 실행 설정 필요 지원되는 서비스에 사용 가능 (현재 Network Load Balancer 및 Application Load Balancer)
고객 주도	고객 주도	AWS주도

라우팅 제어	영역 전환	영역 자동 전환
트래픽을 재라우팅할 시점을 고객이 결정합니다.	영역 전환을 시작할 시점을 고객이 결정합니다.	AWS 사용자를 대신하여 애플리케이션 트래픽을 AZ에서 다른 곳으로 이동합니다.
수수료 기반 라우팅 제어에는 별도의 요금 필요	서비스에 포함 지원되는 로드 밸런서에 트래픽을 AZ에서 다른 곳으로 이동하기 위해 영역 전환을 생성하는 기능 포함	서비스에 포함 지원되는 로드 밸런서에 트래픽을 AZ에서 다른 곳으로 이동하기 위해 사용자 대신 자동 영역 전환을 시작하는 기능 포함
만료되지 않음 트래픽은 복제본으로 무기한 재라우팅 가능	임시 모든 영역 전환은 만료되도록 설정해야 함	임시 AWS 자동 변속 시작 및 종료

이러한 각 기능에 대한 자세한 내용은 다음 장을 참조하세요.

- Amazon Route 53 Application Recovery Controller의 영역 전환
- Amazon Route 53 Application Recovery Controller의 영역 자동 전환
- Amazon Route 53 Application Recovery Controller의 라우팅 제어

Amazon Route 53 애플리케이션 복구 컨트롤러에서 영역 이동 및 영역 자동 이동을 사용하여 애플리케이션을 복구합니다.

이 섹션에서는 Amazon Route 53 애플리케이션 복구 컨트롤러의 기능을 사용하여 가용 영역 (AZ) 의 문제로부터 AWS 애플리케이션을 안정적으로 복구하는 방법을 설명합니다. 이러한 기능인 영역 이동 및 영역 자동 이동은 Elastic Load Balancing 리소스를 위해 트래픽을 일시적으로 AZ에서 다른 곳으로 이동시켜 애플리케이션 복구 시간을 단축합니다.

영역 이동과 영역 자동 이동의 주요 차이점은 하나는 사용자가 제어하는 수동 트래픽 이동이고 다른 하나는 사용자를 대신하여 자동으로 트래픽을 장애에서 멀어지게 이동한다는 것입니다.

- 영역 이동을 사용하면 관리형 Elastic Load Balancing 리소스의 트래픽을 AWS 리전 가용 영역에서 다른 곳으로 수동으로 이동합니다.
- 영역 자동 이동을 사용하면 Elastic Load Balancing 트래픽이 이벤트 중에 사용자를 대신하여 장애가 발생한 AZ에서 정상 상태의 AZ로 자동으로 이동합니다.

다음 항목에서는 영역 이동 및 영역 자동 이동 기능과 사용 방법을 설명합니다.

주제

Amazon Route 53 Application Recovery Controller의 영역 전환

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동을 사용하면 Elastic Load Balancing 리소스의 트래픽을 an의 가용 영역에서 다른 곳으로 이동하여 문제를 신속하게 완화하고 애플리케이션을 빠르게 복구할 수 있습니다. AWS 리전이 기능을 사용하려면 Elastic Load Balancing 리소스에서 영역 간 로드 밸런싱을 해제해야 한다는 점에 유의하세요.

한 지역의 여러 AZ에 있는 로드 밸런서에 AWS 애플리케이션을 배포하고 실행하는 경우 영역 이동을 시작하여 손상된 AZ의 애플리케이션을 빠르게 복구할 수 있습니다. 애플리케이션 트래픽을 정상 AZ로 전환하면 AZ의 정전 또는 하드웨어 또는 소프트웨어 문제로 인한 영향의 지속 기간과 심각도를 줄일 수 있습니다.

예를 들어 잘못된 배포로 인해 지연 문제가 발생하거나 가용 영역이 손상되어 트래픽을 이동할 수 있습니다. 영역 이동에는 사전 구성 단계가 필요하지 않지만, AWS 구성에서 가용 영역을 변경하지 않고도 클라이언트 부하를 처리할 수 있어야 합니다. 지원되는 로드 밸런서 리소스는 Amazon Route 53 애플리케이션 복구 컨트롤러에 자동으로 등록되므로 필요할 때 로드 밸런서의 영역 이동을 간단히 시작할 수 있습니다.

영역 이동을 시작할 때는 설정이나 구성이 필요하지 않습니다. 트래픽을 가용 영역 밖으로 이동할 수 있을 만큼 충분한 용량이 확보되었는지 확인한 후, 이동할 가용 영역과 트래픽을 다른 곳으로 이동할 리소스를 선택한 다음 영역 이동을 시작하십시오. 언제든지 전환을 취소하여 트래픽이 가용 영역으로 돌아오기 시작할 수 있습니다.

모든 영역 이동은 일시적인 완화 조치입니다. 구역 이동을 시작할 때 최초 만료를 1시간에서 최대 3일(72시간) 까지 설정하며, 교통 이동을 계속해야 하는 경우 이 기간을 연장할 수 있습니다.

몇 가지 특정 시나리오에서는 영역 이동으로 인해 AZ의 트래픽이 이동되지 않는다는 점에 유의하십시오. 영역 전환에 대한 자세한 내용은 영역 전환 및 영역 자동 전환에 지원되는 리소스 섹션을 참조하세요.

영역 전환이 작동하는 방식

로드 밸런서 리소스의 영역 이동을 시작하면 해당 리소스의 트래픽이 지정된 가용 영역에서 멀어집니다. 전환을 시작하기 위해 Amazon Route 53 애플리케이션 복구 컨트롤러는 가용 영역을 비정상으로 설정하기 위한 로드 밸런서 상태 점검을 요청하여 상태 확인에 실패하게 합니다. 비정상 상태 점검으로 인해 Amazon Route 53은 DNS에서 리소스의 해당 IP 주소를 자동으로 철회하여 트래픽이 가용 영역에서 리디렉션됩니다. 이제 새 연결이 대신 다른 가용 영역으로 라우팅됩니다. AWS 리전

중요한 점은 영역 이동에서는 상태 점검이 로드 밸런서 또는 애플리케이션의 기본 상태를 모니터링하는 일반적인 방식으로는 상태 확인을 사용하지 않는다는 점입니다. 대신 Route 53 ARC는 상태 확인을 메커니즘으로 사용하여 트래픽을 가용 영역에서 멀어지게 합니다. 이 메커니즘은 트래픽 흐름 방식을 변경하기 위해 상태 확인을 명시적으로 비정상으로 설정했다가 다시 정상으로 설정하도록 요청합니다.

트래픽 이동 시작 - Route 53 ARC에서 영역 이동을 시작하면 트래픽 흐름과 관련된 단계 때문에 트래픽이 가용 영역 밖으로 즉시 이동하지 않을 수 있습니다. 또한 클라이언트 동작과 연결 재사용에 따라 가용 영역에서 진행 중인 기존 연결이 완료되는 데 다소 시간이 걸릴 수 있습니다. DNS 설정 및 기타 요인에 따라 기존 연결은 단 몇 분 만에 완료될 수도 있고 더 오래 걸릴 수도 있습니다. 자세한 내용은 트래픽 이동이 빠르게 완료되도록 하기를 참조하십시오.

트래픽 이동 종료 - 구역 이동이 만료되거나 사용자가 이를 취소하면 Route 53 ARC는 트래픽 이동을 중지하기 위한 조치를 취합니다. 트래픽 이동 시작 프로세스를 되돌리고 Route 53 상태 점검을 다시 정

상으로 설정하도록 요청합니다. 상태 점검이 정상이면 원래 영역 IP 주소가 복원됩니다. 이제 복구된 가용 영역이 다시 로드 밸런서의 라우팅에 포함되고 트래픽이 AZ로 다시 흐르기 시작합니다.

이동을 시작할 때 모든 영역 이동이 만료되도록 설정해야 합니다. 처음에 영역 전환이 최대 3일(72시간) 후에 만료되도록 설정할 수 있습니다. 하지만 언제든지 영역 전환을 업데이트하여 새 만료를 설정할 수 있습니다. 가용 영역으로 트래픽을 복원할 준비가 되면 만료되기 전에 영역 전환을 취소할 수도 있습니다.

교통체증이 사라지지 않는 경우

몇 가지 특정 시나리오에서는 영역 전환으로 인해 AZ의 트래픽이 이동되지 않습니다. 예를 들어 AZ의 로드 밸런서 대상 그룹에 인스턴스가 없거나 모든 인스턴스가 비정상인 경우 로드 밸런서는 페일 오픈 상태에 있습니다. 이 시나리오에서 로드 밸런서에 대한 영역 전환을 시작하는 경우 로드 밸런서가 이미 페일 오픈 상태이므로 로드 밸런서가 사용하는 AZ는 변경되지 않습니다. 이는 예상된 동작입니다. 영역 전환은 모든 AZ가 페일 오픈(비정상)인 경우 한 AZ를 강제로 비정상 상태로 만들고 트래픽을 한 리전의 다른 AZ로 이동시킬 수 없습니다. 두 번째 시나리오는 AWS Global Accelerator에서 액셀러레이터의 엔드포인트인 Application Load Balancer의 영역 전환을 시작하는 경우입니다. 글로벌 액셀러레이터에서 액셀러레이터의 엔드포인트인 Application Load Balancer에는 영역 전환이 지원되지 않습니다.

영역 전환에 대한 자세한 내용은 영역 전환 및 영역 자동 전환에 지원되는 리소스 섹션을 참조하세요.

AWS 리전 구역 이동 가능 여부

Amazon Route 53 Application Recovery Controller의 리전 지원 및 서비스 엔드포인트에 대한 자세한 내용은 Amazon Web Services 일반 참조의 Amazon Route 53 Application Recovery Controller 엔드포인트 및 할당량을 참조하세요.

구역 이동은 현재 여기 AWS 리전 목록에서 확인할 수 있습니다. 영역 전환은 중국 리전(중국(베이징) 리전 및 중국(닝샤) 리전)에서 사용 가능합니다.

리전 이름	지역	엔드포인트	프로토콜	
미국 동부(오하이오)	us-east-2	arc-zonal-shift.us-east-2.amazonaws.com	HTTPS	
미국 동부(버지니아 북부)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS	

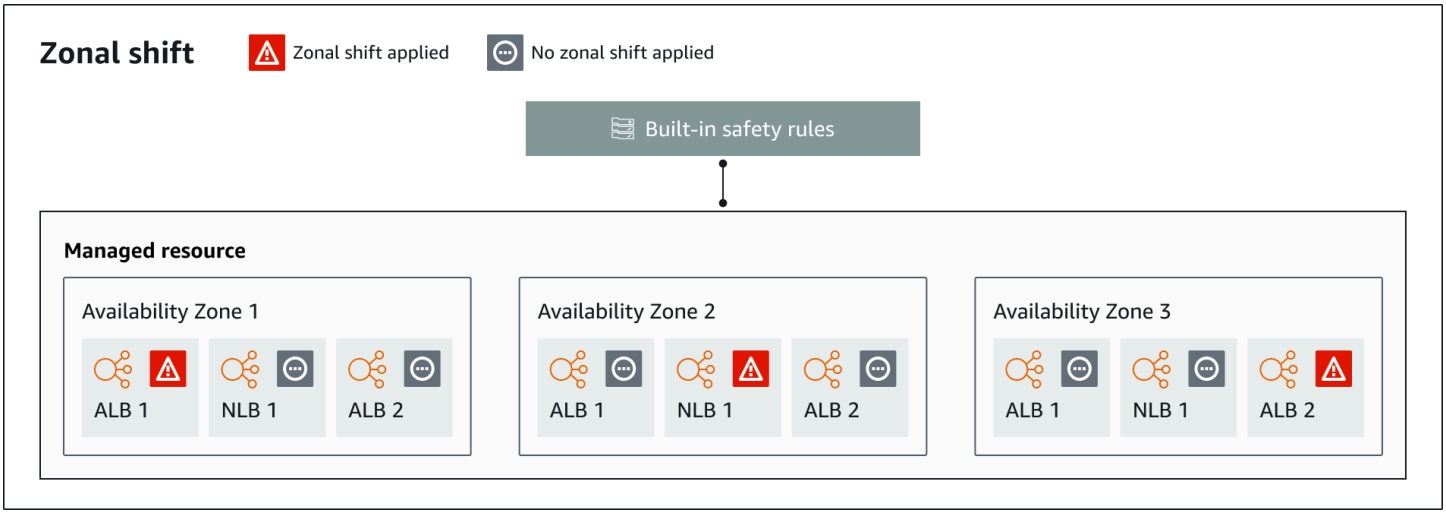
리전 이름	지역	엔드포인트	프로토콜	
미국 서부(캘리포니아 북부)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS	
미국 서부(오레곤)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS	
아프리카(케이프타운)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS	
아시아 태평양(홍콩)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS	
아시아 태평양(하이데라바드)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS	
아시아 태평양(자카르타)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com	HTTPS	
아시아 태평양(멜버른)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com	HTTPS	
아시아 태평양(뭄바이)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com	HTTPS	
아시아 태평양(오사카)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com	HTTPS	

리전 이름	지역	엔드포인트	프로토콜	
아시아 태평양(서울)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com	HTTPS	
아시아 태평양(싱가포르)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com	HTTPS	
아시아 태평양(시드니)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com	HTTPS	
아시아 태평양(도쿄)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS	
캐나다(중부)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS	
캐나다 서부(캘거리)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS	
유럽(프랑크푸르트)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS	
유럽(아일랜드)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS	
유럽(런던)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS	
유럽(밀라노)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS	
유럽(파리)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com	HTTPS	

리전 이름	지역	엔드포인트	프로토콜	
유럽(스페인)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com	HTTPS	
유럽(스톡홀름)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com	HTTPS	
유럽(취리히)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com	HTTPS	
이스라엘(텔아비브)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com	HTTPS	
중동(바레인)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com	HTTPS	
중동(UAE)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com	HTTPS	
남아메리카(상파울루)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com	HTTPS	
AWS GovCloud(미국 동부)	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com	HTTPS	
AWS GovCloud(미국 서부)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com	HTTPS	

영역 전환 구성 요소

다음 다이어그램은 트래픽이 가용 영역에서 멀어지는 영역 이동의 예를 보여줍니다. AWS 리전영역 이동에 내장된 검사 기능을 사용하면 리소스에 이미 활성 상태인 리소스의 영역 이동을 다시 시작할 수 없습니다.



Route 53 ARC의 영역 이동 기능 구성 요소는 다음과 같습니다.

영역 전환

AWS 계정의 관리 리소스에 대한 영역 전환을 시작하여 한 AZ의 문제를 신속하게 복구하기 위해 일시적으로 트래픽을 해당 지역의 가용 영역에서 멀어지는 정상 AZ로 이동합니다. AWS 리전현재는 영역 간 로드 밸런싱이 구성되지 않은 Network Load Balancer 및 Application Load Balancer에 대해서만 영역 전환을 시작할 수 있습니다. 지원되는 로드 밸런서는 Route 53 ARC에 자동으로 등록됩니다.

내장된 안전 검사

Route 53 ARC에 내장된 검사는 리소스에 대한 트래픽 이동이 한 번에 두 번 이상 적용되지 않도록 합니다. 즉, 고객 주도 영역 전환, 연습 실행 영역 전환 또는 리소스의 자동 전환 한 번만이 트래픽을 가용 영역 밖으로 능동적으로 전환시킬 수 있습니다. 예를 들어, 현재 자동 전환으로 다른 곳으로 전환된 리소스에 영역 전환을 시작하면 영역 전환이 우선 적용됩니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller의 영역 자동 전환 및 연습 실행 결과를 참조하세요.

리소스 식별자

영역 전환에 포함할 리소스의 식별자. 리소스 식별자는 Amazon 리소스 이름(ARN)입니다.

영역 이동의 경우 Route 53 ARC에서 지원하는 AWS 서비스의 계정에서 리소스만 선택할 수 있습니다. 해당 AWS 서비스에서 지원되는 리소스는 서비스에 의해 Route 53 ARC에 AWS 자동으로 등록됩니다.

> **Note**
>
> 현재는 영역 간 로드 밸런싱이 해제된 네트워크 로드 밸런서 및 애플리케이션 로드 밸런서에 대해서만 영역 이동을 시작할 수 있습니다.

관리 리소스

AWS 서비스는 영역 이동을 위해 Route 53 ARC에 리소스를 자동으로 등록합니다. 등록된 리소스는 Route 53 ARC의 관리 리소스입니다.

리소스 이름

영역 이동을 위해 지정할 수 있는 Route 53 ARC의 리소스 이름입니다.

상태(영역 전환 상태)

영역 전환의 상태입니다. 영역 전환에 대한 `Status`에는 다음 값 중 하나가 포함될 수 있습니다.

- ACTIVE: 영역 전환이 시작되고 활성화됩니다.
- EXPIRED: 영역 전환이 만료되었습니다(만료 시간이 초과됨).
- CANCELED: 영역 전환이 취소되었습니다.

적용 상태

적용된 상태는 리소스에 전환이 적용되는지 여부를 나타냅니다. 상태가 지정된 이동에 따라 리소스에 대한 애플리케이션 트래픽이 이동된 가용 영역과 해당 이동이 종료되는 시기가 `APPLIED` 결정됩니다.

만료 시간(만료 시간)

영역 전환에 대한 만료 시간입니다. 영역 전환은 일시적입니다. 고객 주도 영역 전환의 경우 처음에 영역 전환이 최대 3일(72시간) 동안 활성화되도록 설정할 수 있습니다.

영역 전환을 시작할 때 활성화할 기간을 지정하면 Route 53 ARC가 만료 시간(만료 시간)으로 변환합니다. 예를 들어 가용 영역으로 트래픽을 복원할 준비가 되면 고객 주도 영역 전환을 취소할 수 있습니다. 또는 다른 만료 시간을 지정하도록 업데이트하여 고객 주도 영역 전환을 연장할 수 있습니다.

영역 자동 전환으로 연습을 실행하는 경우 고객이 시작한 영역 이동과 AWS 시작한 영역 이동을 모두 취소할 수 있습니다.

구역 이동을 위한 데이터 및 제어 플레인

페일오버와 재해 복구를 계획할 때는 페일오버 메커니즘이 얼마나 탄력적인지 생각해 보세요. 재해 시나리오에서 필요할 때 사용할 수 있도록 페일오버 중에 사용하는 메커니즘의 가용성이 높은지 확인하는 것이 좋습니다. 일반적으로 안정성과 내결함성을 극대화하려면 가능하면 언제든지 메커니즘에 데이터 플레인 함수를 사용해야 합니다. 이를 염두에 두고 서비스의 기능이 컨트롤 플레인과 데이터 영역 간에 어떻게 구분되는지, 그리고 서비스의 데이터 영역에서 최상의 신뢰성을 기대할 수 있는 경우를 이해하는 것이 중요합니다.

대부분의 AWS 서비스와 마찬가지로 영역 이동 기능 기능은 컨트롤 플레인 및 데이터 플레인에서 지원됩니다. 둘 다 신뢰성을 위해 구축되었지만 컨트롤 플레인은 데이터 일관성을 위해 최적화되고 데이터 플레인은 가용성을 위해 최적화됩니다. 데이터 영역은 복원력을 고려하여 설계되었으므로 컨트롤 플레인 사용이 불가능해질 수 있는 운영 중단에도 가용성을 유지할 수 있습니다.

일반적으로 컨트롤 플레인을 사용하면 서비스의 리소스 생성, 업데이트 및 삭제와 같은 기본 관리 기능을 수행할 수 있습니다. 데이터 영역은 서비스의 핵심 기능을 제공합니다.

데이터 플레인, 컨트롤 플레인, 고가용성 목표를 달성하기 위해 서비스를 AWS 구축하는 방법에 대한 자세한 내용은 Amazon Builders' Library의 가용 영역을 사용한 정적 안정성 문서를 참조하십시오.

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 변경 요금

영역 이동의 경우, 지원되는 리소스의 영역 이동을 시작하여 가용 영역의 문제로부터 애플리케이션을 복구할 수 있습니다. 영역 전환을 사용해도 추가 요금이 부과되지 않습니다.

Amazon Route 53 애플리케이션 복구 컨트롤러에서 사용한 만큼만 비용을 지불하면 됩니다. Route 53 ARC에 대한 자세한 요금 정보와 요금 예제를 보려면 Amazon Route 53 요금을 참조하고 아래로 스크롤하여 Amazon Route 53 애플리케이션 복구 컨트롤러로 이동하십시오.

Route 53 ARC의 영역 전환 모범 사례

Route 53 ARC에서 다중 AZ 복구를 위한 영역 전환에 대한 권장 모범 사례입니다. 영역 전환은 일반적으로 라이브 애플리케이션의 용량을 제거하므로 프로덕션 환경에서 사용할 때는 주의해야 합니다.

주제

- 용량 계획 및 사전 조정
- 클라이언트가 엔드포인트에 연결된 상태를 유지하는 시간을 제한하세요.
- 시작 영역 이동을 미리 테스트하세요.
- 모든 가용 영역이 정상이고 트래픽을 받고 있는지 확인하세요.
- 재해 복구에 데이터 플레인 API 작업을 사용하십시오.
- 영역 이동이 있는 트래픽은 일시적으로만 이동합니다.

용량 계획 및 사전 규모 조정

영역 전환을 시작할 때 가용 영역에 부과되는 추가 부하를 수용할 수 있는 충분한 용량을 계획하고 사전 규모 조정 또는 자동 확장이 가능한지 확인합니다. 복구 지향 아키텍처에서는 일반적으로 세 개의 복제본 중 하나가 오프라인 상태일 때 최대 트래픽을 처리할 수 있는 충분한 여유 공간을 포함하도록 컴퓨팅 용량을 미리 조정하는 것이 좋습니다.

예를 들어 단일 로드 밸런서 리소스의 영역 전환을 시작하면 한 가용 영역의 용량이 로드 밸런서 뒤에서 일시적으로 제거됩니다. 시작하는 영역 전환과 로드 밸런서의 구성 방식에 따라 나머지 가용 영역에서 증가된 부하 관리를 신중하게 계획했는지 확인해야 합니다.

클라이언트가 엔드포인트에 연결된 상태를 유지하는 시간을 제한하세요.

Amazon Route 53 애플리케이션 복구 컨트롤러가 영역 이동 또는 영역 자동 이동을 사용하는 등 장애가 발생하지 않는 곳으로 트래픽을 이동할 때 Route 53 ARC가 애플리케이션 트래픽을 이동하는 데 사용하는 메커니즘은 DNS 업데이트입니다. DNS 업데이트로 인해 모든 새 연결이 손상된 위치에서 멀어집니다.

그러나 기존 연결이 열려 있는 클라이언트는 클라이언트가 다시 연결될 때까지 손상된 위치에 대해 요청을 계속할 수 있습니다. 빠른 복구를 위해 클라이언트가 엔드포인트에 연결된 상태를 유지하는 시간을 제한하는 것이 좋습니다.

Application Load Balancer를 사용하는 경우 `keepalive` 옵션을 사용하여 연결 지속 시간을 구성할 수 있습니다. 자세한 내용은 Application Load Balancer 사용 설명서의 HTTP 클라이언트 유지 기간을 참조하십시오.

기본적으로 애플리케이션 로드 밸런서는 HTTP 클라이언트 keepalive 기간 값을 3600초 또는 1시간으로 설정합니다. 애플리케이션의 복구 시간 목표 (예: 300초) 에 맞도록 값을 낮추는 것이 좋습니다. HTTP 클라이언트 keepalive 지속 시간을 선택할 때는 일반적으로 재연결을 더 자주 하는 것이 지연 시간에 영향을 줄 수 있는 것과 손상된 AZ 또는 지역에서 모든 클라이언트를 더 빨리 멀리 이동시키는 것 사이의 절충점이라는 점을 고려하세요.

시작 영역 이동을 미리 테스트해 보세요.

영역 전환을 시작하여 애플리케이션의 가용 영역 밖으로 트래픽을 이동하는 것을 정기적으로 테스트합니다. 재해 발생 시 애플리케이션 복구를 위한 정기적인 장애 조치 테스트의 일환으로 가급적이면 테스트 및 프로덕션 환경 모두에서 시작 영역 전환을 계획하고 실행합니다. 정기적인 테스트는 운영상 문제가 발생했을 때 문제를 완화할 수 있는 대비와 확신을 갖도록 하는 데 있어 매우 중요한 부분입니다.

모든 가용 영역이 정상이고 트래픽을 받고 있는지 확인하세요.

영역 전환은 가용 영역에서 리소스, 즉 애플리케이션 복제본을 비정상으로 표시함으로써 작동합니다. 즉, 애플리케이션의 로드 밸런서에 있는 대상이 일반적으로 정상이고 리전 내 가용 영역에서 트래픽을 적극적으로 받아들이는지 확인하는 것이 중요합니다. 비정상 대상에 대한 Elastic Load Balancing 지표 및 가용 영역당 처리된 바이트 수를 포함하여 이를 추적할 수 있는 대시보드를 사용하는 것이 좋습니다.

인접한 두 번째 지역에서 리소스 상태를 모니터링하는 것을 고려해 보십시오. 이 접근 방식의 장점은 최종 사용자의 경험을 더 잘 대표할 수 있고 애플리케이션과 모니터링이 동시에 동일한 재해로 인해 영향을 받는 위험(“운명 공유”)을 줄일 수 있다는 것입니다.

재해 복구에는 데이터 플레인 API 작업을 사용하십시오.

종속성이 거의 없는 애플리케이션을 신속하게 복구해야 할 때 영역 이동을 시작하려면 가능한 경우 사전 저장된 자격 증명과 함께 영역 이동 작업이 포함된 AWS Command Line Interface 또는 API를 사용하는 것이 좋습니다. 사용하기 쉽도록 에서 영역 이동을 시작할 수도 있습니다. AWS Management Console그러나 빠르고 안정적인 복구가 중요한 경우에는 데이터 영역 작업을 선택하는 것이 좋습니다. 자세한 내용은 영역 전환 API 참조 안내서를 참조하세요.

구역 이동을 통한 트래픽 이동은 일시적으로만 가능합니다.

영역 전환은 장애를 완화하기 위해 트래픽을 일시적으로 가용 영역 밖으로 이동시킵니다. 문제를 해결하기 위한 조치를 취하는 즉시 애플리케이션이 서비스를 받을 수 있도록 리소스를 복원해야 합니다. 이를 통해 전체 애플리케이션이 완전히 중복되고 복원력이 뛰어난 원래의 상태로 복원될 수 있습니다.

영역 전환 API 작업

다음 표에는 다중 AZ 애플리케이션의 가용 영역 밖으로 트래픽을 이동시키는 영역 전환으로 사용할 수 있는 Route 53 ARC API 작업이 나열되어 있습니다. 이 표에는 관련 문서에 대한 링크도 포함되어 있습니다.

AWS Command Line Interface에서 일반적인 영역 전환 API 작업을 사용하는 방법에 대한 예는 영역 이동과 AWS CLI 함께 사용하는 예 섹션을 참조하세요.

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
영역 전환 시작	영역 전환 시작 섹션 참조	Shift 참조 StartZonal
영역 전환 업데이트	영역 전환 업데이트 또는 취소 섹션 참조	UpdateZonal쉬프트 참조
영역 전환 나열	Amazon Route 53 Application Recovery Controller의 영역 전환 섹션 참조	ListZonal교대 근무 참조
관리 리소스 나열	영역 전환 및 영역 자동 전환에 지원되는 리소스 섹션 참조	리소스 보기 ListManaged
관리 리소스 가져오기	영역 전환 및 영역 자동 전환에 지원되는 리소스 섹션 참조	GetManaged리소스 참조
영역 전환 취소	영역 전환 업데이트 또는 취소 섹션 참조	CancelZonal쉬프트 참조

영역 이동과 AWS CLI 함께 사용하는 예

이 섹션에서는 API 작업을 사용하는 Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동 기능을 사용하기 AWS Command Line Interface 위해 영역 이동을 사용하는 간단한 애플리케이션 예제를 살펴봅니다. 이 예제는 CLI를 사용하여 영역 이동 작업을 수행하는 방법에 대한 기본적인 이해를 돕기 위한 것입니다.

Route 53 ARC의 영역 이동을 사용하면 지원되는 리소스의 트래픽을 일시적으로 가용 영역에서 다른 가용 영역으로 이동하여 애플리케이션이 다른 가용 영역과 함께 정상적으로 계속 작동할 수 있습니다. AWS 리전현재 영역 전환은 영역 간 로드 밸런싱이 꺼진 상태의 Network Load Balancer 및 Application Load Balancer를 지원됩니다.

AWS Command Line Interface를 사용하여 영역 전환을 시작하는 예를 살펴보겠습니다. AWS CLI 를 사용하여 영역 전환을 업데이트할 수도 있습니다(예: 새 만료 설정). 모든 영역 전환은 일시적이므로 처음에는 3일 이내에 만료되도록 설정해야 합니다. 하지만 나중에 영역 전환을 업데이트하여 새 만료를 설정할 수 있습니다.

사용에 대한 자세한 내용은 명령 AWS CLI참조를 참조하십시오.AWS CLI 영역 전환 API 작업 목록 및 자세한 정보 링크는 영역 전환 API 작업 섹션을 참조하세요.

영역 전환 시작

`start-zonal-shift` 명령을 사용하여 CLI에서 영역 전환을 시작할 수 있습니다.

```
aws arc-zonal-shift start-zonal-shift \
      --resource-identifier="arn:aws:testservice::111122223333:ExampleALB123456890" \
      --away-from="usw2-az1" \
      --expires-in="5m" \
      --comment="Shifting traffic away from USW2-AZ1"
```

```
{
   "zonalShiftId": "2222222-3333-444-1111",
   "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
   "awayFrom": "usw2-az1",
   "expiryTime": 2022-11-14T01:40:42+00:00,
   "startTime": 2022-11-14T01:35:42+00:00,
   "status": "ACTIVE",
   "comment": "Shifting traffic away from USW2-AZ1"
}
```

관리 리소스 가져오기

`get-managed-resource` 명령을 사용하여 CLI에서 관리 리소스에 대한 정보를 가져올 수 있습니다.

```
aws arc-zonal-shift get-managed-resource \
   --resource-identifier="arn:aws:testservice::111122223333:ExampleALB123456890
```

```
{
    "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "name": "TestResource",
    "appliedWeights": {
        "usw2-az1": 1.0,
        "usw2-az2": 1.0,
        "usw2-az3": 1.0
    },
    "zonalShifts": []
}
```

관리 리소스 나열

`list-managed-resources` 명령을 사용하여 CLI에서 계정의 관리 리소스를 나열할 수 있습니다.

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

```
{
    "items": [
        {
            "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
            "name": "TestResource",
            "availabilityZones": [
                "usw2-az1",
                "usw2-az2",
                "usw2-az3"
            ]
        }
    ]
}
```

영역 전환 목록

`list-zonal-shifts` 명령을 사용하여 CLI를 통해 계정의 영역 전환을 나열할 수 있습니다.

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

```
{
    "items": [
        {
            "zonalShiftId": "2222222-3333-444-1111",
            "resourceIdentifier":
 "arn:aws:testservice::111122223333:ExampleALB123456890",
            "awayFrom": "usw2-az1",
            "expiryTime": 2022-11-15T09:10:42+00:00,
            "startTime": 2022-11-13T01:35:42+00:00,
            "status": "ACTIVE",
            "comment": "Shifting traffic away from USW2-AZ1"
        }
    ]
}
```

영역 전환 업데이트

update-zonal-shift 명령을 사용하여 CLI로 영역 전환을 업데이트할 수 있습니다.

```
aws arc-zonal-shift update-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890" \
   --expires-in="1h" \
   --comment="Still shifting traffic away from USW2-AZ1"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2022-11-15T10:35:42+00:00,
    "startTime": 2022-11-15T09:35:42+00:00,
    "status": "ACTIVE",
    "comment": "Still shifting traffic away from USW2-AZ1"
}
```

영역 전환 취소

cancel-zonal-shift 명령을 사용하여 CLI에서 영역 전환을 취소할 수 있습니다.

```
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": 2022-11-15T10:35:42+00:00,
    "startTime": 2022-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Shifting traffic away from USW2-AZ1"
}
```

영역 전환 및 영역 자동 전환에 지원되는 리소스

Amazon Route 53 애플리케이션 복구 컨트롤러는 현재 영역 이동 및 영역 자동 이동을 위한 다음 리소스를 지원합니다.

- Network Load Balancers
- Application Load Balancers

지원되는 로드 밸런싱 리소스는 Route 53 ARC에 자동으로 등록되므로 영역 이동 (및 영역 자동 이동)과 함께 사용할 수 있습니다. Elastic Load Balancing 콘솔 (대부분 AWS 리전) 또는 Route 53 ARC에서 로드 밸런서의 영역 이동을 시작할 수 있습니다.

Route 53 ARC에서 영역 전환 및 리소스 작업을 위한 다음 조건을 검토합니다.

- 영역 전환에서는 교차 영역 로드 밸런싱이 지원되지 않습니다. Route 53 ARC에 로드 밸런서를 등록하려면 Elastic Load Balancing에서 로드 밸런서에 대한 영역 간 로드 밸런싱을 해제해야 합니다.
- 몇 가지 특정 시나리오에서는 영역 이동으로 인해 AZ에서 들어오는 트래픽이 이동하지 않습니다. 예를 들어 AZ의 로드 밸런서 대상 그룹에 인스턴스가 없거나 모든 인스턴스가 비정상인 경우 로드 밸런서는 페일 오픈 상태이며 AZ 중 하나에서 전환할 수 없습니다.
- 공용 및 내부(사설) Network Load Balancer와 Application Load Balancer가 모두 지원됩니다.
- 트래픽을 이동하려면 리소스가 활성 상태이고 완전히 프로비저닝되어야 합니다. 리소스의 영역 전환을 시작하기 전에 해당 리소스가 Route 53 ARC에서 관리되는 리소스인지 확인합니다. 예를 들어 에서 관리 리소스 목록을 보거나 리소스 식별자와 함께 `get-managed-resource` 작업을 사용할 수 있습니다. AWS Management Console
- AWS Global Accelerator의 엔드포인트인 Application Load Balancer에는 영역 전환이 지원되지 않습니다.
- Network Load Balancer의 대상인 Application Load Balancer는 Network Load Balancer에서 영역 전환을 시작합니다. Application Load Balancer에서 영역 전환을 시작하는 경우 Network Load Balancer는 Application Load Balancer 및 해당 대상으로의 트래픽 전송을 중지합니다.
- 영역 이동을 위한 리소스는 AWS 서비스가 Route 53 ARC에 등록한 관리형 리소스여야 합니다. Elastic Load Balancing은 교차 영역 로드 밸런싱이 꺼진 상태에서 Route 53 ARC Network Load Balancer 및 Application Load Balancer에 자동으로 등록합니다.
- 리소스를 사용하여 영역 이동을 시작하려면 해당 리소스를 가용 영역과 이동을 시작하는 AWS 리전 위치에 배포해야 합니다. 전환 대상 AZ가 속한 리전과 동일한 리전에서 영역 전환을 시작하고 트래픽을 이동하려는 리소스도 동일한 AZ 및 리전에 있어야 합니다.
- 리소스에서 영역 전환을 사용하려면 올바른 IAM 권한이 있는지 확인해야 합니다. 자세한 정보는 영역 전환을 위한 IAM 및 권한을 참조하세요.

영역 이동 시작, 업데이트 또는 취소

이 섹션에서는 구역 이동 시작 및 취소를 포함하여 구역 이동 작업을 위한 절차를 제공합니다.

영역 전환 시작

이 섹션의 단계에서는 Amazon Route 53 Application Recovery Controller 콘솔에서 고객 주도 영역 전환을 시작하는 방법을 설명합니다. 프로그래밍 방식으로 영역 전환 작업을 수행하려면 영역 전환 API 참조 안내서를 참조하세요.

Route 53 ARC에서 영역 이동을 시작하는 것 외에도 Elastic Load Balancing 콘솔 (지원되는 지역) 에서 로드 밸런서의 영역 이동을 시작할 수도 있습니다. 자세한 내용은 Elastic Load Balancing 사용 설명서의 영역 이동을 참조하십시오.

영역 전환 시작

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 다중 AZ에서 영역 전환을 선택합니다.
3. 영역 전환 페이지에서 영역 전환 시작을 선택합니다.
4. 트래픽을 이동할 가용 영역을 선택합니다.
5. 리소스 테이블에서 트래픽을 다른 곳으로 옮길 로드 밸런서를 선택합니다.
6. 영역 전환 만료 설정에서 영역 전환 만료를 선택하거나 입력합니다. 영역 전환은 처음에 1분부터 최대 3일(72시간)까지 활성화되도록 설정할 수 있습니다.

   모든 영역 전환은 일시적입니다. 만료를 설정해야 하지만 나중에 활성 전환을 업데이트하여 최대 3일의 만료 기간을 새로 설정할 수 있습니다.
7. 설명을 입력합니다. 원하는 경우 나중에 영역 전환을 업데이트하여 설명을 편집할 수 있습니다.
8. 영역 전환을 시작하면 트래픽을 해당 가용 영역에서 다른 곳으로 이동하여 애플리케이션의 사용 가능한 용량이 줄어든다는 것을 확인하려면 확인란을 선택합니다.
9. 시작을 선택합니다.

영역 전환 업데이트 또는 취소

이 섹션의 단계에서는 Amazon Route 53 Application Recovery Controller 콘솔에서 직접 시작한 영역 전환을 업데이트 또는 취소하는 방법을 설명합니다. 프로그래밍 방식으로 영역 전환 작업을 수행하려면 영역 전환 API 참조 안내서를 참조하세요.

영역 전환을 업데이트하여 새 만료를 설정하거나 영역 전환에 대한 설명을 편집 또는 대체할 수 있습니다. 영역 전환은 만료되기 전에 언제든지 취소할 수 있습니다.

영역 자동 이동을 위한 연습 실행의 경우 시작한 영역 이동 또는 리소스에 대해 AWS 시작하는 영역 이동을 취소할 수 있습니다. 영역 자동 이동의 연습 교대에 대한 자세한 내용은 을 참조하십시오. 영역 자동 전환 및 연습 실행의 작동 방식

영역 전환 업데이트

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 다중 AZ에서 영역 전환을 선택합니다.
3. 업데이트하려는 영역 전환을 선택한 다음 영역 전환 업데이트를 선택합니다.
4. 영역 전환 만료 설정에서 만료를 선택하거나 입력할 수 있습니다.
5. Comment(설명)의 경우 기존 설명을 편집하거나 새 설명을 입력할 수 있습니다.
6. 업데이트를 선택합니다.

영역 전환 취소

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 다중 AZ에서 영역 전환을 선택합니다.
3. 취소하려는 영역 전환을 선택한 다음 영역 전환 취소를 선택합니다.
4. 확인 모달 대화 상자에서 확인을 선택합니다.

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동에 대한 로깅 및 모니터링

AWS CloudTrail 및 Amazon을 사용하여 Amazon EventBridge Route 53 애플리케이션 복구 컨트롤러의 영역 이동을 모니터링하여 패턴을 분석하고 문제를 해결할 수 있습니다.

주제

- 를 사용하여 영역 이동 API 호출 로깅 AWS CloudTrail
- Amazon에서 영역 이동 사용하기 EventBridge

를 사용하여 영역 이동 API 호출 로깅 AWS CloudTrail

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 전환은 Route 53 ARC에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 기록을 제공하는 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail 영역 이동에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Route 53 ARC 콘솔에서의 통화와 영역 이동을 위한 Route 53 ARC API 작업에 대한 코드 호출이 포함됩니다.

트레일을 생성하면 영역 이동 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다.

에서 수집한 CloudTrail 정보를 사용하여 영역 이동을 위해 Route 53 ARC에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

구역 이동 정보: CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. 영역 이동으로 인해 Route 53 ARC에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. AWS 계정자세한 내용은 CloudTrail 이벤트 기록 작업을 참조하십시오.

Route 53 ARC의 지역 이동 이벤트를 포함하여 해당 지역의 지속적인 이벤트 기록을 보려면 트레일을 생성하십시오 AWS 계정. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Route 53 ARC 작업은 Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 가이드에 의해 CloudTrail 기록되고 문서화되어 있습니다. 예를 들어, `StartZonalShift` 및 `ListManagedResources` 작업에 대한 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail UserIdentity 요소를 참조하십시오.

이벤트 기록에서 Route 53 ARC 이벤트 확인하기

CloudTrail 이벤트 기록에서 최근 이벤트를 볼 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록 작업을 참조하십시오.

구역 이동 로그 파일 항목의 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 영역 이동 `ListManagedResources` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.


```
{
      "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"
      }
    }
```


다음 예제는 영역 이동에 대한 충돌 예외가 있는 `StartZonalShift` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.


```
{
      "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"
      }
    }
```


Amazon에서 영역 이동 사용하기 EventBridge

EventBridgeAmazon을 사용하면 영역 이동 리소스를 모니터링하고 다른 서비스를 사용하는 목표 조치를 시작하는 이벤트 기반 규칙을 설정할 수 있습니다. AWS 예를 들어 영역 이동이 시작될 때 Amazon SNS 주제에 신호를 보내 이메일 알림을 보내는 규칙을 설정할 수 있습니다.

Amazon에서 규칙을 EventBridge 생성하여 영역 이동에 적용할 수 있습니다. 영역 이동 이벤트는 영역 이동에 대한 상태 정보를 지정합니다. 예를 들어 구역 이동을 시작하면 이벤트가 생성됩니다.

관심 있는 특정 영역 이동 이벤트를 캡처하려면 이벤트를 감지하는 데 사용할 EventBridge 수 있는 이벤트별 패턴을 정의하십시오. 이벤트 패턴은 일치하는 이벤트와 동일한 구조를 갖습니다. 패턴은 일치시키려는 필드를 인용하고 찾고 있는 값을 제공합니다.

이벤트는 최선의 작업을 기반으로 발생됩니다. 정상적인 운영 EventBridge 환경에서는 Route 53 ARC에서 거의 실시간으로 전송됩니다. 하지만 이벤트 전달을 지연하거나 방해하는 상황이 발생할 수 있습니다.

EventBridge 규칙이 이벤트 패턴과 함께 작동하는 방식에 대한 자세한 내용은 의 이벤트 및 이벤트 패턴을 참조하십시오 EventBridge.

다음을 통해 영역 이동 리소스를 모니터링하세요. EventBridge

를 사용하면 Route 53 ARC가 리소스에 대한 이벤트를 내보낼 때 취할 조치를 정의하는 규칙을 생성할 수 있습니다. EventBridge 예를 들어 영역 이동을 시작할 때 이메일 메시지를 보내는 규칙을 생성할 수 있습니다.

이벤트 패턴을 입력하거나 복사하여 콘솔에 붙여넣으려면 EventBridge 콘솔에서 Enter my own 옵션을 사용하는 옵션을 선택합니다. 유용할 수 있는 이벤트 패턴을 결정하는 데 도움이 되도록 이 항목에는 영역 이동 이벤트 일치 패턴의 예가 포함되어 있습니다.

리소스 이벤트에 대한 규칙을 만들려면

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 규칙을 생성하려는 대상, 즉 이벤트를 시청하고 싶은 지역을 선택합니다. AWS 리전
3. Create rule을 선택합니다.
4. 규칙의 이름을 입력하고 선택적으로 설명을 입력합니다.
5. 이벤트 버스의 경우 기본값을 그대로 두세요.
6. 다음을 선택합니다.
7. 이벤트 패턴 빌드 단계에서 이벤트 소스의 경우 기본값인 AWS 이벤트를 그대로 두세요.
8. 샘플 이벤트에서 직접 입력을 선택합니다.
9. 샘플 이벤트에 이벤트 패턴을 입력하거나 복사하여 붙여넣습니다.

Route 53 ARC 이벤트 패턴 예

이벤트 패턴은 일치하는 이벤트와 동일한 구조를 갖습니다. 패턴은 일치시키려는 필드를 인용하고 찾고 있는 값을 제공합니다.

- Route 53 ARC 구역 이동에서 모든 이벤트를 선택합니다.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ]
}
```

대상으로 사용할 CloudWatch 로그 그룹을 지정합니다.

규칙을 만들 때는 EventBridge 규칙과 일치하는 이벤트가 전송되는 대상을 지정해야 합니다. 사용 가능한 대상 EventBridge 목록은 EventBridge 콘솔에서 사용 가능한 대상을 참조하십시오. EventBridge 규칙에 추가할 수 있는 대상 중 하나는 Amazon CloudWatch 로그 그룹입니다. 이 섹션에서는 CloudWatch 로그 그룹을 대상으로 추가하기 위한 요구 사항을 설명하고 규칙을 생성할 때 로그 그룹을 추가하는 절차를 제공합니다.

CloudWatch 로그 그룹을 대상으로 추가하려면 다음 중 하나를 수행할 수 있습니다.

- 새 로그 그룹 생성
- 기존 로그 그룹 선택

규칙을 생성할 때 콘솔을 사용하여 새 로그 그룹을 지정하면 이 EventBridge 자동으로 로그 그룹을 생성합니다. EventBridge 규칙의 대상으로 사용하는 로그 그룹이 로 시작하는지 확인하십시오/aws/events. 기존 로그 그룹을 선택하려는 경우 로 시작하는 로그 그룹만 드롭다운 메뉴에 옵션으로 /aws/events 표시된다는 점에 유의하세요. 자세한 내용은 Amazon CloudWatch 사용 설명서의 새 로그 그룹 생성을 참조하십시오.

콘솔 외부의 CloudWatch 작업을 사용하여 대상으로 사용할 CloudWatch 로그 그룹을 만들거나 사용하는 경우 권한을 올바르게 설정해야 합니다. 콘솔을 사용하여 EventBridge 규칙에 로그 그룹을 추가하면 해당 로그 그룹의 리소스 기반 정책이 자동으로 업데이트됩니다. 그러나 AWS Command Line Interface 또는 AWS SDK를 사용하여 로그 그룹을 지정하는 경우 로그 그룹에 대한 리소스 기반 정책을 업데이트해야 합니다. 다음 예제 정책은 리소스 기반 정책에서 로그 그룹에 정의해야 하는 권한을 보여줍니다.

```
{
  "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"
}
```

콘솔을 사용하여 로그 그룹에 대한 리소스 기반 정책을 구성할 수는 없습니다. 리소스 기반 정책에 필요한 권한을 추가하려면 API 작업을 사용하십시오. CloudWatch PutResourcePolicy 그런 다음 describe-resource-policiesCLI 명령을 사용하여 정책이 올바르게 적용되었는지 확인할 수 있습니다.

리소스 이벤트에 대한 규칙을 생성하고 CloudWatch 로그 그룹 대상을 지정하려면

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 규칙을 AWS 리전 생성하려는 항목을 선택합니다.
3. 규칙 생성을 선택한 다음 해당 규칙에 대한 정보 (예: 이벤트 패턴 또는 일정 세부 정보) 를 입력합니다.

   Route 53 ARC용 EventBridge 규칙 생성에 대한 자세한 내용은 이 주제 앞부분의 섹션을 참조하십시오.
4. 대상 선택 페이지에서 CloudWatch대상으로 선택합니다.
5. 드롭다운 메뉴에서 CloudWatch 로그 그룹을 선택합니다.

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동을 위한 Identity 및 Access Management

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. AWS IAM 관리자는 누가 Route 53 ARC 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

내용

영역 이동이 IAM과 함께 작동하는 방식

Amazon Route 53 애플리케이션 복구 컨트롤러에서 IAM을 사용하여 영역 이동에 대한 액세스를 관리하기 전에 영역 이동과 함께 사용할 수 있는 IAM 기능에 대해 알아보십시오.

영역 이동과 함께 사용할 수 있는 IAM 기능

IAM 특성	영역 이동 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 보안 인증	예
보안 주체 권한	예

IAM 특성	영역 이동 지원
서비스 역할	아니요
서비스 링크 역할	예

AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 개괄적으로 파악하려면 IAM 사용 설명서의 IAM과 연동되는AWS 서비스를 참조하십시오.

Route 53 ARC의 자격 증명 기반 정책

ID 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Route 53 ARC 자격 증명 기반 정책의 예를 보려면 Amazon Route 53 애플리케이션 복구 컨트롤러의 ID 기반 정책 예제 섹션을 참조하세요.

Route 53 ARC 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다.

영역 이동을 위한 정책 조치

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

영역 이동에 대한 Route 53 ARC 작업 목록을 보려면 서비스 권한 부여 참조의 Amazon Route 53 영역 이동에서 정의한 작업을 참조하십시오.

영역 이동을 위한 Route 53 ARC의 정책 조치는 조치 전에 다음 접두사를 사용합니다.

```
arc-zonal-shift
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다. 예를 들면 다음과 같습니다.

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

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `Describe`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

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

영역 이동에 대한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동에 대한 ID 기반 정책 예제

영역 이동을 위한 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

리소스 유형 및 해당 ARN 목록과 각 리소스의 ARN으로 지정할 수 있는 작업을 보려면 서비스 권한 부여 참조의 다음 항목을 참조하십시오.

- 아마존 Route 53에서 정의한 작업 - 영역 이동

조건 키와 함께 사용할 수 있는 작업 및 리소스를 보려면 서비스 권한 부여 참조의 다음 항목을 참조하십시오.

- Amazon Route 53에서 정의한 조건 키 - 영역 이동

영역 이동에 대한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동에 대한 ID 기반 정책 예제

영역 이동을 위한 정책 조건 키

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition요소를 지정하거나 단일 Condition요소에서 여러 키를 지정하는 경우 AWS 는 논리적 AND태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

영역 이동 조건 키 목록을 보려면 서비스 권한 부여 참조의 다음 주제를 참조하십시오.

- Amazon Route 53에서 정의한 조건 키 - 영역 이동

조건 키와 함께 사용할 수 있는 작업 및 리소스를 보려면 서비스 권한 부여 참조에서 다음 항목을 참조하세요.

- 아마존 Route 53에서 정의한 작업 - 영역 이동
- Amazon Route 53에서 정의한 리소스 유형 - 영역 이동

영역 이동에 대한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동에 대한 ID 기반 정책 예제

Route 53 ARC의 액세스 제어 목록(ACL)

ACL 지원	아니요

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Route 53 ARC과 함께하는 ABAC(속성 기반 액세스 제어)

ABAC(정책 내 태그) 지원	부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Route 53 ARC에는 ABAC에 대한 다음과 같은 부분 지원이 포함됩니다.

- 영역 전환은 영역 전환을 위해 Route 53 ARC에 등록된 관리형 리소스에 대해 ABAC를 지원합니다. Network Load Balancer용 ABAC 및 Application Load Balancer에서 관리되는 리소스에 대한 자세한 내용은 Elastic Load Balancing 사용 설명서에서 Elastic Load Balancer를 사용하는 ABC를 참조하세요.

Route 53 ARC에서 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

Route 53 ARC의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원	예

IAM 개체 (사용자 또는 역할) 를 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 정책은 보안 주체에게 권한을 부여합니다. 일부 서비스를 사용할 때는 다른 서비스에서 다른 작업을 트리거하는 작업을 수행할 수 있습니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다.

작업에 정책의 종속 작업이 추가로 필요한지 알아보려면 서비스 권한 부여 참조의 다음 주제를 참조하십시오.

- Amazon Route 53 영역 전환

Route 53 ARC의 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조합니다.

Route 53 ARC의 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

영역 이동은 서비스 연결 역할을 사용하지 않습니다.

영역 전환을 위한 IAM 및 권한

이 섹션에서는 Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동 기능에 대한 권한 작동 방식에 대한 추가 정보를 제공합니다. 특히 Elastic Load Balancing과 같은 다른 AWS 서비스에서 해당 기능을 사용하는 경우 더욱 그렇습니다. Route 53 ARC 기능이 IAM 및 권한과 함께 일반적으로 어떻게 작동하는지 알아보려면 개요 항목의 정보를 검토하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동을 위한 Identity 및 Access Management

IAM 개요 항목에 설명된 권한 외에도 IAM 및 권한의 영역 이동에는 다음이 적용됩니다.

- Route 53 ARC에서 영역 전환 작업에 필요한 권한이 있는지 확인합니다. 자세한 내용은 영역 이동 콘솔 액세스 및 영역 이동 운영 액세스를 참조하십시오.
- Route 53 ARC에서 계정의 관리형 로드 밸런서 리소스의 영역 전환 작업을 위해 IAM에 Elastic Load Balancing 권한을 추가할 필요가 없습니다.
- Elastic Load Balancing에 대한 전체 액세스를 제공하는 AWS 관리형 정책에는 영역 이동 작업에 대한 권한이 포함됩니다. Elastic Load Balancing 액세스에 AWS 관리형 정책을 사용하는 경우, 로드 밸런서의 영역 이동을 시작하거나 Elastic Load Balancing 콘솔에서 작업할 때 영역 이동에 대한 IAM의 추가 권한이 필요하지 않습니다. 자세한 내용은 Elastic Load Balancing AWS 관리형 정책을 참조하세요.

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동에 대한 ID 기반 정책 예제

기본적으로 사용자 및 역할에는 Route 53 ARC 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 API를 사용하여 작업을 수행할 수 없습니다. AWS 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 비롯하여 Route 53 ARC에 의해 정의되는 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 Amazon Route 53 Application Recovery Controller에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례

- 예: Zonal Shift 콘솔 액세스
- 예: 영역 이동 API 작업

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Route 53 ARC 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

예: Zonal Shift 콘솔 액세스

Amazon Route 53 Application Recovery Controller 콘솔에 액세스하려면 최소한의 권한 세트가 있어야 합니다. 이러한 권한을 통해 내 Route 53 ARC 리소스를 나열하고 세부 정보를 볼 수 있어야 AWS 계정 합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자에게 영역 이동을 사용할 수 있는 모든 권한을 부여하려면 다음과 같은 정책을 사용자에게 첨부하세요. AWS Management Console

```
{
    "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": "*"
        }
    ]
}
```

예: 영역 이동 API 작업

영역 이동 API는 애플리케이션을 복구하기 위해 트래픽을 일시적으로 가용 영역에서 다른 곳으로 이동 합니다.

사용자가 영역 이동 API 작업을 사용할 수 있도록 하려면 다음과 같이 사용자가 작업해야 하는 API 작업에 해당하는 정책을 첨부하세요.

```
{
    "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": "*"
        }
    ]
}
```

Amazon Route 53 Application Recovery Controller의 영역 자동 전환

영역 자동 이동을 사용하면 이벤트 발생 시 사용자 대신 애플리케이션의 리소스 트래픽을 가용 영역에서 다른 곳으로 이동시켜 AWS 복구 시간을 단축할 수 있습니다. AWS 내부 원격 분석 결과 고객에게 잠재적으로 영향을 미칠 수 있는 가용 영역 장애가 있는 것으로 확인되면 자동 전환을 시작합니다. 자동 전환을 AWS 시작하면 영역 자동 이동을 위해 구성한 리소스로 향하는 애플리케이션 트래픽이 가용 영역에서 멀어지기 시작합니다.

Route 53 ARC는 개별 리소스의 상태를 검사하지 않는다는 점에 유의하십시오. AWS AWS 원격 분석으로 고객에게 잠재적으로 영향을 미칠 수 있는 가용 영역 장애가 감지되면 자동 전환을 시작합니다. 영향을 받지 않는 리소스로 트래픽이 이동하는 경우도 있습니다.

또한 영역 자동 이동을 사용하면 정기적인 AWS 연습 실행 시 사용자 대신 애플리케이션의 리소스 트래픽을 가용 영역에서 다른 곳으로 이동할 수 있습니다. 영역 자동 전환에는 연습 실행이 필요합니다. Route 53 ARC가 연습 실행을 위해 시작하는 영역 전환은 자동 전환 중에 가용 영역에서 트래픽을 다른 곳으로 이동하는 것이 애플리케이션에 안전한지 확인하는 데 도움이 됩니다. 연습 실행은 리소스의 트래픽을 가용 영역 밖으로 이동시키는 영역 전환을 시작하여 가용 영역 하나가 없어도 애플리케이션이 정상적으로 작동할 수 있는지 정기적으로 테스트합니다. 실습은 매주 진행되며 애플리케이션이 예상대로 작동하는지 파악하는 FAILED 데 도움이 되는 결과 (예: SUCCEEDED 또는) 를 제공합니다.

> **Important**
>
> 실습을 구성하거나 영역 자동 전환을 활성화하기 전에 애플리케이션 리소스가 배포되는 지역의 모든 가용 영역에서 애플리케이션 리소스 용량을 미리 스케일링하는 것이 좋습니다. 자동 전환 또는 연습 실행이 시작될 때 온디맨드 크기 조정에만 의존해서는 안 됩니다. 연습 실행을 포함한 영역 자동 전환은 독립적으로 작동하며 Auto Scaling 작업이 완료될 때까지 기다리지 않습니다. 사전 조정 대신 Auto Scaling을 사용하면 애플리케이션 복구 시간이 더 오래 걸릴 수 있습니다.
>
> Auto Scaling을 사용하여 정기적인 트래픽 주기를 처리하는 경우, 가용 영역이 손실되어도 계속 정상적으로 작동하도록 Auto Scaling의 최소 용량을 구성하는 것이 좋습니다.

영역 자동 이동을 활성화하거나 연습 실행을 구성하려는 경우 애플리케이션 리소스 용량을 사전 조정한 후 가용 영역이 하나도 없어도 애플리케이션이 정상적으로 작동할 수 있는지 테스트하십시오. 이를 테스트하려면 영역 전환을 시작하여 리소스의 트래픽을 가용 영역 밖으로 이동시키세요.

영역 이동을 사용한 테스트가 효과적인지 확인하려면 이전한 AZ에서 트래픽이 예상대로 소모되는지 확인하는 것이 중요합니다. 애플리케이션 로드 밸런서와 네트워크 로드 밸런서 모두 Amazon에서 이를 모니터링하는 데 사용할 수 CloudWatch 있는 AZ별 지표를 제공합니다. 서비스와 클라이언트가 연결을 재사용하는 기간에 따라 이동한 트래픽이 AZ에 예상보다 오래 지속될 수 있습니다. 자세히 알아보려면 클라이언트가 엔드포인트에 연결된 상태로 유지되는 시간 제한을 참조하십시오.

영역 이동을 시작하고 평가하여 트래픽이 가용 영역에서 멀어져도 애플리케이션이 정상적으로 계속 작동할 수 있는지 확인한 후, Route 53 ARC가 수행하는 정기 연습 실행을 통해 자동 전환을 위한 충분한 용량이 있는지 지속적으로 확인할 수 있습니다.

Route 53 ARC 콘솔에서 로드 밸런서 리소스의 영역 자동 이동을 활성화하는 것 외에도 Amazon EC2 콘솔에서 특정 로드 밸런서에 대해 영역 자동 이동을 활성화하는 옵션이 있습니다. Elastic Load Balancing으로 영역 자동 이동을 활성화하는 방법에 대해 자세히 알아보려면 Elastic Load Balancing 사용 설명서의 영역 이동을 참조하십시오.

자동 전환 및 연습 실행 영역 전환은 일시적입니다. 자동 시프트를 사용하면 영향을 받는 가용 영역이 복구되면 리소스 트래픽이 가용 영역 밖으로 이동하는 것을 AWS 중지합니다. 리전의 모든 가용 영역에 고객의 애플리케이션 트래픽이 반환됩니다. 연습 실행 시 트래픽은 약 30분 동안 단일 리소스의 가용 영역에서 이동했다가 다시 해당 리전의 모든 가용 영역으로 돌아옵니다.

자동 변속 및 연습 실행에 대해 알리도록 Amazon EventBridge 알림을 구성할 수 있습니다. 자세한 정보는 Amazon에서 영역 자동 변속 사용하기 EventBridge을 참조하세요.

영역 자동 전환 및 연습 실행의 작동 방식

Amazon Route 53 Application Recovery Controller의 영역 자동 이동 기능을 사용하면 AWS 가용 영역에서 고객에게 잠재적으로 영향을 미칠 수 있는 장애가 있다고 AWS 판단될 때 사용자를 대신하여 리소스의 트래픽을 가용 영역 밖으로 이동할 수 있습니다. 영역 자동 전환은 한 가용 영역 내의 모든 가용 영역에서 사전 조정되는 리소스를 위해 설계되었으므로 하나의 AWS 리전가용 영역이 손실되더라도 애플리케이션이 정상적으로 작동할 수 있습니다.

영역 자동 전환을 사용하면 Route 53 ARC가 리소스에 대한 트래픽을 한 가용 영역에서 다른 곳으로 정기적으로 이동하는 연습 실행을 구성해야 합니다. Route 53 ARC는 연습 실행 구성이 연결된 각 리소스에 대해 대략 매주 연습 실행을 예약합니다. 각 리소스에 대한 연습 실행은 독립적으로 예약됩니다.

Route 53 ARC는 각 연습 실행의 결과를 기록합니다. 차단 조건으로 인해 연습 실행이 중단되는 경우 연습 실행 결과는 성공으로 표시되지 않습니다. 연습 실행 결과에 대한 자세한 내용은 연습 실행 결과를 참조하세요.

자동 변속 및 연습 실행에 대한 정보를 보내도록 Amazon EventBridge 알림을 구성할 수 있습니다. 자세한 정보는 Amazon에서 영역 자동 변속 사용하기 EventBridge을 참조하세요.

주제

자동 변속 AWS 시작 및 중지 시점

리소스에 대한 영역 자동 이동을 활성화하면 복구 시간을 AWS 단축하기 위해 이벤트 중에 애플리케이션의 리소스 트래픽을 가용 영역에서 이동하도록 사용자를 대신하여 권한을 부여합니다.

이를 위해 zonal autoshift는 AWS 원격 분석을 사용하여 고객에게 잠재적으로 영향을 미칠 수 있는 가용 영역 장애를 최대한 빨리 탐지합니다. AWS 가 자동 전환을 시작하면 구성된 리소스로의 트래픽이 고객에게 잠재적으로 영향을 미칠 수 있는 손상된 가용 영역에서 즉시 벗어나기 시작합니다.

영역 자동 전환은 모든 가용 영역에 맞게 애플리케이션 리소스를 사전 조정한 고객을 위해 설계된 기능입니다. AWS 리전자동 전환 또는 연습 실행이 시작될 때 온디맨드 크기 조정에만 의존해서는 안 됩니다.

AWS 가용 영역이 복구되었다고 판단되면 자동 전환을 종료합니다.

Route 53 ARC가 연습 실행을 예약, 시작 및 종료하는 시점

Route 53 ARC는 매주 약 30분 동안 리소스에 대한 연습 실행을 예약합니다. Route 53 ARC는 각 리소스에 대한 연습 실행을 개별적으로 예약, 시작 및 관리합니다. Route 53 ARC는 동일한 계정의 리소스에 대한 연습 실행을 배치 처리하지 않습니다.

연습 실행이 중단 없이 예상 기간 동안 계속되면 결과가 `SUCCESSFUL`로 표시됩니다. 그 외에도 `FAILED`, `INTERRUPTED`, `PENDING`과 같은 결과가 나올 수 있습니다. 결과 값과 설명은 연습 실행 결과 섹션에 포함되어 있습니다.

Route 53 ARC가 연습 실행을 중단하고 종료하는 몇 가지 시나리오가 있습니다. 예를 들어 연습 실행 중에 자동 전환이 시작되면 Route 53 ARC는 연습 실행을 중단하고 종료합니다. 또 다른 예로, 리소스가 연습 실행에 부정적인 반응을 보여 연습 실행을 모니터링하도록 지정한 경보가 `ALARM` 상태로 전환된다고 가정해 보겠습니다. 이 시나리오에서도 Route 53 ARC는 연습 실행을 중단하고 종료합니다.

또한 Route 53 ARC가 리소스에 예약된 연습 실행을 시작하지 않는 몇 가지 시나리오가 있습니다.

리소스에 대한 연습 실행이 중단되고 차단되면 Route 53 ARC는 다음을 수행합니다.

- 리소스에 대한 연습 실행이 진행 중에 중단되면 Route 53 ARC는 주간 연습 실행이 끝난 것으로 간주하고 다음 주로 해당 리소스에 대한 새로운 연습 실행을 예약합니다. 이 시나리오에서 주간 연습 결과는 `FAILED`가 아닌 `INTERRUPTED`입니다. 연습 실행 결과는 연습 실행을 모니터링하는 결과 경보가 연습 실행 중에 `ALARM` 상태가 될 때만 `FAILED`로 설정됩니다.
- 리소스에 대한 연습 실행이 시작되도록 예약되어 있을 때 차단 제약이 있는 경우 Route 53 ARC는 연습 실행을 시작하지 않습니다. Route 53 ARC는 여전히 하나 이상의 차단 제약이 있는지 확인하기 위해 정기적인 모니터링을 계속합니다. 차단 제약이 없는 경우 Route 53 ARC는 리소스에 대한 연습 실행을 시작합니다.

다음은 Route 53 ARC가 리소스에 대한 연습 실행을 시작하거나 계속하지 못하도록 차단하는 제약 조건의 예입니다.

- Route 53 ARC는 AWS Fault Injection Service 실험이 진행 중인 경우 연습 실행을 시작하거나 계속하지 않습니다. Route 53 ARC가 연습 실행을 시작하도록 예약했을 때 AWS FIS 이벤트가 활성화된 경우 Route 53 ARC는 연습 실행을 시작하지 않습니다. Route 53 ARC는 연습 실행 내내

AWS FIS 이벤트를 포함한 차단 제약 조건을 모니터링합니다. 연습 실행이 활성화된 상태에서 AWS FIS 이벤트가 시작되면 Route 53 ARC는 연습 실행을 종료하고 리소스에 대해 정기적으로 예정된 다음 연습 실행이 있을 때까지 다른 연습을 시작하려고 시도하지 않습니다.

- 지역에 현재 AWS 이벤트가 있는 경우 Route 53 ARC는 해당 지역에서 리소스에 대한 연습 실행을 시작하지 않고 진행 중인 연습 실행을 종료합니다.

연습 실행이 중단되지 않고 끝나면 Route 53 ARC는 평소와 같이 일주일 후에 다음 연습 실행을 예약합니다. 지정한 AWS FIS 실험 또는 차단된 시간 창과 같은 차단 제약 때문에 연습 실행이 시작되지 않는 경우, Route 53 ARC는 연습 실행을 시작할 수 있을 때까지 연습 실행을 계속 시도합니다.

영역 전환, 연습 실행 및 자동 전환의 우선순위

한 번에 적용되는 리소스의 트래픽 이동은 한 번을 초과할 수 없습니다. 즉, 해당 리소스에 대해 연습 실행, 고객 주도 영역 전환 또는 자동 전환을 한 번만 실행할 수 있습니다. 진행 중인 트래픽 전환이 두 개 이상인 경우 Route 53 ARC는 우선순위에 따라 리소스에 적용되는 트래픽 전환을 결정합니다.

우선 순위에 대한 전반적인 원칙은 고객으로서 시작한 구역 이동이 연습 실행보다 우선하는 자동 이동보다 우선한다는 것입니다. 즉, 고객 주도하는 영역 전환 > 자동 전환 > 연습 실행 영역 전환의 순서입니다.

이를 설명하기 위해 아래에 몇 가지 예시 시나리오에서 우선순위가 어떻게 작용하는지가 나와 있습니다.

- 활성화된 자동 전환이 있고 자동 전환이 활성화된 리소스에 대해 영역 전환을 시작하는 경우 직접 시작하는 영역 전환이 `APPLIED` 상태가 됩니다. 이제 리소스는 영역 전환이 적용되는 가용 영역에서 다른 곳으로 이동됩니다. AWS 가 자동 전환을 종료하기 전에 영역 전환이 종료되면 자동 전환이 `APPLIED` 상태가 됩니다. 따라서 자동 전환이 진행 중인 가용 영역에서 리소스가 다른 곳으로 이동합니다. AWS
- 자동 전환이 활성화된 리소스에 대해 활성 영역 이동을 시작했는데 자동 전환이 AWS 시작되면 해당 리소스에 대한 자동 전환이 존재합니다. 하지만 영역 전환은 `APPLIED` 상태로 설정되고 자동 전환은 영역 전환이 종료될 때까지 `NOT APPLIED` 상태로 설정됩니다. 그러면 자동 전환 상태가 로 업데이트되고 자동 전환은 자동 전환이 `APPLIED` 종료될 때까지 리소스를 향해 트래픽을 다른 곳으로 이동시킵니다. AWS
- 리소스에 대한 연습 실행이 진행 중이고 동일한 가용 영역으로부터 트래픽을 이동시키도록 해당 리소스에 영역 전환을 시작하면 연습 실행이 중단됩니다. 트래픽을 다른 가용 영역에서 다른 곳으로 이동시키는 영역 전환을 시작하면 연습 실행은 평소와 같이 계속됩니다.
- 리소스에 대한 영역 전환이 활성화되어 있고 Route 53 ARC가 연습 실행을 시작하도록 예약되어 있는 경우 연습 실행은 한 시간 연기됩니다. 그런 다음 Route 53 ARC가 다시 연습 실행을 시작하

려고 시도합니다. Route 53 ARC는 연습 실행을 시작할 수 있을 때까지 매시간 계속해서 검사합니다.

현재 리소스에 적용되는 트래픽 전환에는 적용된 영역 전환 상태가 APPLIED로 설정되어 있습니다. 한 번에 한 번의 전환만 APPLIED로 설정됩니다. 진행 중인 다른 전환은 ACTIVE로 설정됩니다.

리소스에 대한 활성 자동 전환 또는 연습 실행 중지

리소스에 대해 진행 중인 자동 전환을 중지하려면 해당 리소스의 영역 자동 전환을 비활성화하세요.

영역 자동 전환을 비활성화해도 리소스의 연습 실행 구성은 영향을 받지 않습니다. 리소스에 대한 정기적인 연습 실행은 여전히 동일한 일정에 따라 진행됩니다. 자동 전환을 비활성화하는 데 더해 연습 실행을 중지하려면 리소스와 관련된 연습 실행 구성을 삭제해야 합니다.

연습 실행 구성을 삭제하면 매주 해당 리소스의 트래픽을 가용 영역 밖으로 이동하는 연습 실행이 AWS 중지됩니다. 또한 영역 자동 전환에는 연습 실행이 필요하므로 Route 53 ARC 콘솔을 사용하여 연습 실행 구성을 삭제하면 리소스의 영역 자동 전환도 비활성화됩니다. 하지만 영역 자동 전환 API를 사용하여 연습 실행을 삭제하는 경우 먼저 리소스의 영역 자동 전환을 비활성화해야 합니다.

활성 연습 실행을 중지하려면 영역 전환 연습 실행을 취소하세요. 자세한 정보는 연습 실행 영역 전환 취소을 참조하세요.

트래픽이 다른 곳으로 전환되는 방법

자동 전환 및 연습 실행 영역 전환의 경우 Route 53 ARC가 고객 주도 영역 전환에 사용하는 것과 동일한 메커니즘을 사용하여 트래픽이 가용 영역에서 다른 곳으로 이동합니다. 영역 간 로드 밸런싱이 꺼진 로드 밸런서의 트래픽을 가용 영역 밖으로 이동시키기 위해 Route 53 ARC는 가용 영역에 대한 로드 밸런서 상태 확인을 비정상으로 설정하여 상태 확인에 실패합니다. 결과적으로 비정상적인 상태 확인으로 인해 Amazon Route 53가 DNS에서 해당 리소스의 IP 주소를 철회하여 트래픽이 가용 영역에서 리디렉션됩니다. 이제 새 연결이 AWS 리전 대신 다른 가용 영역으로 라우팅됩니다.

자동 전환을 사용하면 가용 영역이 복구되고 자동 전환을 AWS 종료하기로 결정하면 Route 53 ARC는 상태 확인 프로세스를 역으로 되돌려 Route 53 상태 확인을 되돌릴 것을 요청합니다. 그러면 원래 영역 IP 주소가 복원되고 상태 확인이 계속 정상이면 가용 영역이 로드 밸런서의 라우팅에 다시 포함됩니다.

자동 전환은 로드 밸런서 또는 애플리케이션의 기본 상태를 모니터링하는 상태 확인을 기반으로 하지 않는다는 점에 유의해야 합니다. Route 53 ARC는 상태 확인을 비정상으로 설정하도록 요청하고, 자동 전환 또는 영역 전환을 종료하면 상태 확인을 다시 정상으로 복원함으로써 상태 확인을 사용하여 트래픽을 가용 영역 밖으로 이동시킵니다.

연습 실행 경보

영역 자동 전환으로 연습을 실행하는 경우 두 개의 CloudWatch 경보를 지정할 수 있습니다. 첫 번째 경보인 결과 경보는 필수입니다. 30분 간격의 연습 실행 때마다 트래픽이 가용 영역에서 벗어날 때 애플리케이션의 상태를 모니터링하도록 결과 경보를 구성해야 합니다.

효과적인 연습 실행을 위해 리소스 또는 애플리케이션의 메트릭을 모니터링하는 CloudWatch 경보를 결과 경보로 지정하십시오. 이 경보는 가용 영역 하나가 손실되어 애플리케이션이 부정적인 영향을 받을 때 ALARM 상태로 응답합니다. 자세한 내용은 영역 자동 이동을 구성할 때의 모범 사례의 연습 실행에 지정하는 경보 섹션을 참조하세요.

결과 경보는 Route 53 ARC가 각 연습 실행에 대해 보고하는 연습 실행 결과에 대한 정보도 제공합니다. 경보가 ALARM 상태에 들어가면 연습 실행이 종료되고 연습 실행 결과가 FAILED로 반환됩니다. 연습 실행이 30분간의 예정된 테스트 기간을 마치고 결과 경보가 ALARM 상태로 전환되지 않는 경우 결과는 SUCCEEDED으로 반환됩니다. 모든 결과 값 목록과 설명은 연습 실행 결과 섹션에 나와 있습니다.

선택적으로 두 번째 경보인 차단 경보를 지정할 수 있습니다. 차단 경보는 연습 실행이 ALARM 상태일 때 연습 실행이 시작되거나 계속되는 것을 차단합니다. 이 경보는 경보가 ALARM 상태일 때 연습 실행 트래픽 전환이 시작되지 않도록 차단하고 진행 중인 모든 연습 실행을 중지합니다.

예를 들어 마이크로서비스가 여러 개 있는 대규모 아키텍처에서 한 마이크로서비스에 문제가 발생하면 대개 연습 실행 차단을 포함하여 애플리케이션 환경의 다른 모든 변경을 중지하기를 원합니다.

차단 날짜 및 차단 기간(UTC)

특정 날짜 또는 특정 기간, 즉 요일과 시간(UTC)의 연습 실행을 차단할 수 있는 옵션이 있습니다.

예를 들어, 2024년 5월 1일에 애플리케이션 업데이트가 출시될 예정인데 이때 연습 실행으로 인해 트래픽이 다른 곳으로 이동하는 것을 원하지 않는 경우 차단 날짜를 2024-05-01로 설정하면 됩니다.

또는 일주일에 3일 비즈니스 보고서 요약을 실행한다고 가정해 보겠습니다. 이 시나리오에서는 MON-20:30-21:30 WED-20:30-21:30 FRI-20:30-21:30(UTC)과 같이 반복되는 요일과 시간을 차단 기간으로 설정할 수 있습니다.

영역 자동 이동에 대한 정보

영역 자동 전환은 사용자를 대신하여 애플리케이션 리소스 트래픽을 가용 영역 밖으로 AWS 이동시키는 기능입니다. AWS 내부 원격 측정 결과 고객에게 잠재적으로 영향을 미칠 수 있는 가용 영역 장애가

있는 것으로 확인되면 자동 전환을 시작합니다. 내부 원격 측정에는 AWS 네트워크, Amazon EC2 및 Elastic Load Balancing 서비스를 비롯한 여러 소스의 지표가 통합되어 있습니다.

자동 영역 전환은 영역 간 로드 밸런싱이 꺼진 상태에서 Application Load Balancer 및 Network Load Balancer에서 활성화할 수 있습니다.

한 지역의 여러 AZ에 있는 로드 밸런서에 AWS 애플리케이션을 배포 및 실행하고 정적 안정성을 지원하도록 사전 규모를 조정하면 자동 전환으로 트래픽을 다른 곳으로 이동시켜 AZ에서 고객 애플리케이션을 빠르게 AWS 복구할 수 있습니다. 리소스 트래픽을 지역 내 다른 AZ로 이동하면 정전, AZ의 하드웨어 또는 소프트웨어 문제 또는 기타 장애로 인한 잠재적 영향의 지속 기간과 심각도를 줄일 AWS 수 있습니다.

로드 밸런싱 리소스에 대한 자동 전환을 AWS 시작하면 Route 53 ARC는 로드 밸런서 리소스의 해당 IP 주소에 대해 Amazon Route 53 상태 확인을 비정상으로 설정하여 리소스의 트래픽이 더 이상 AZ로 전달되지 않도록 합니다. AZ가 애플리케이션 트래픽을 반환할 준비가 되었다고 AWS 판단되면 Route 53 ARC는 Route 53 상태 확인을 복원하고 원래 영역 IP 주소를 복원합니다.

리소스에 대한 영역 자동 이동을 활성화하는 경우 해당 리소스에 대한 연습 실행도 구성해야 합니다. AWS 약 매주 30분 동안 실습을 수행하여 해당 지역의 가용 영역 없이도 애플리케이션을 실행할 수 있는 충분한 용량이 있는지 확인할 수 있도록 도와줍니다.

영역 전환과 마찬가지로 영역 자동 전환으로 인해 트래픽이 AZ에서 이동하지 않는 몇 가지 특정 시나리오가 있습니다. 예를 들어 AZ의 로드 밸런서 대상 그룹에 인스턴스가 없거나 모든 인스턴스가 비정상인 경우 로드 밸런서는 페일 오픈 상태이며 AZ 중 하나에서 전환할 수 없습니다.

영역 자동 전환에 대한 자세한 내용은 Amazon Route 53 Application Recovery Controller의 영역 자동 전환 섹션을 참조하세요.

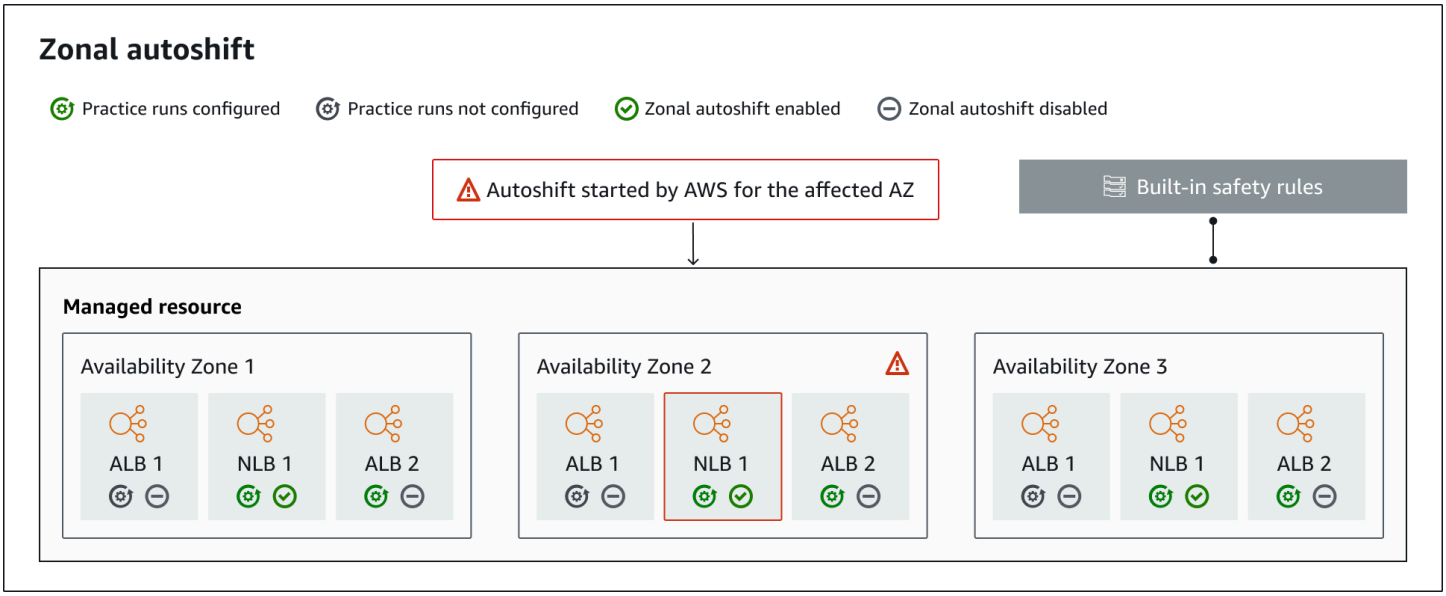
AWS 리전 영역 자동 변속 가능 여부

구역 자동 변속은 현재 상용 버전에서 사용할 수 있습니다. AWS 리전

Amazon Route 53 Application Recovery Controller의 리전 지원 및 서비스 엔드포인트에 대한 자세한 내용은 Amazon Web Services 일반 참조의 Amazon Route 53 Application Recovery Controller 엔드포인트 및 할당량을 참조하세요.

영역 자동 전환 구성 요소

다음 다이어그램은 트래픽을 가용 영역 밖으로 이동시키는 자동 변속의 예를 보여줍니다. AWS 내부 원격 측정 결과 고객에게 잠재적으로 영향을 미칠 수 있는 가용 영역 장애가 있는 것으로 확인되면 자동 전환을 시작합니다.



Route 53 ARC의 영역 자동 전환 기능 구성 요소는 다음과 같습니다.

영역 자동 전환

영역 자동 전환은 별도의 조치를 취하지 않아도 리소스의 트래픽을 전환합니다. 영역 자동 전환은 Route 53 ARC의 기능으로, 내부 원격 측정에서 고객에게 잠재적으로 영향을 미칠 수 있는 가용 영역 장애가 있는 것으로 확인되면 자동 전환을 AWS 시작합니다. 경우에 따라 영향을 받지 않는 리소스가 다른 곳으로 전환될 수 있다는 점에 유의하세요.

연습 실행

리소스에 대해 영역 자동 이동을 활성화하는 경우 해당 리소스에 대한 영역 자동 이동 연습 실행도 구성해야 합니다. AWS 연습을 위해 약 매주, 약 30분 동안 구역 이동을 수행합니다. 연습 실행을 통해 가용 영역 하나가 손실되더라도 애플리케이션이 정상적으로 실행되는지 확인할 수 있습니다. 연습 실행에서는 영역 AWS 이동을 통해 리소스의 트래픽을 한 가용 영역에서 다른 곳으로 이동시킨 다음 연습 실행이 끝나면 트래픽을 다시 이동합니다.

연습 실행 구성

연습 실행 구성은 차단된 날짜와 기간 (있는 경우), 리소스에 대한 연습 실행을 위해 지정하는 CloudWatch 경보를 영역 자동 이동 모드로 정의합니다. 언제든지 연습 실행을 편집하여 차단된 날짜 또는 기간을 추가 또는 변경하거나 연습 실행에 대한 경보를 업데이트할 수 있습니다.

영역 자동 전환을 활성화하려면 리소스에 대한 연습 실행 구성이 있어야 합니다. 연습 실행을 삭제할 수도 있습니다. 리소스의 연습 실행 구성을 삭제하려면 영역 자동 전환을 비활성화해야 합니다.

연습 실행 경보

연습 실행을 구성할 때는 리소스 및 애플리케이션 요구 사항에 따라 생성할 CloudWatch 경보를 지정합니다. CloudWatch 지정하는 경보는 연습 실행으로 인해 애플리케이션이 부정적인 영향을 받는 경우 연습 실행을 시작하지 못하도록 차단하거나 진행 중인 연습 실행을 중지할 수 있습니다.

지정한 경보가 ALARM 상태가 되면 Route 53 ARC는 연습 실행의 영역 전환을 종료하여 리소스의 트래픽이 더 이상 가용 영역에서 다른 곳으로 이동하지 않도록 합니다.

연습 실행에 지정하는 경보에는 두 가지 유형이 있습니다. 하나는 연습 실행 중에 리소스 및 애플리케이션의 상태를 모니터링하는 결과 경보이고, 다른 하나는 연습 실행이 시작되지 않도록 구성하거나 진행 중인 연습 실행을 중지하도록 구성할 수 있는 차단 경보입니다. 결과 경보는 필수이고 차단 경보는 선택 사항입니다.

연습 실행 결과

Route 53 ARC는 각 연습 실행의 결과를 보고합니다. 가능한 연습 실행 결과는 다음과 같습니다.

- 보류 중: 연습 실행의 영역 전환이 활성화되었습니다(진행 중). 아직 반환할 결과가 없습니다.
- 성공: 연습 실행 중에 결과 경보가 ALARM 상태에 들어가지 않았고, 연습 실행이 전체 30분의 테스트 기간을 완료했습니다.
- 중단됨: 결과 경보가 ALARM 상태가 아닌 이유로 연습 실행이 종료되었습니다. 연습 실행은 여러 가지 이유로 중단될 수 있습니다. 예를 들어, 연습 실행에 지정된 차단 경보가 ALARM 상태에 들어갔기 때문에 연습 실행이 종료되는 경우 결과는 INTERRUPTED입니다. INTERRUPTED 결과의 이유에 대한 자세한 내용은 연습 실행 결과를 참조하세요.
- 실패: 연습 실행 중에 결과 경보가 ALARM 상태에 들어갔습니다.

내장된 안전 규칙

Route 53 ARC에 내장된 안전 규칙은 리소스에 대한 트래픽 전환이 한 번에 두 번 이상 적용되지 않도록 합니다. 즉, 고객 주도 영역 전환, 연습 실행 영역 전환 또는 리소스의 자동 전환 한 번만이 트래픽을 가용 영역 밖으로 능동적으로 전환시킬 수 있습니다. 예를 들어, 현재 자동 전환으로 다른 곳으로 전환된 리소스에 영역 전환을 시작하면 영역 전환이 우선 적용됩니다. 자세한 내용은 연습 실행 결과를 참조하십시오.

리소스 식별자

영역 자동 전환을 활성화하는 데 사용할 리소스의 식별자로, 해당 리소스의 Amazon 리소스 이름(ARN) 입니다.

Route 53 ARC에서 지원하는 AWS 서비스에 있는 계정의 리소스에 대해서만 영역 자동 전환을 활성화할 수 있습니다. 해당 AWS 서비스에서 지원되는 리소스는 서비스에 의해 Route 53 ARC에 AWS 자동으로 등록됩니다.

> **Note**
>
> 영역 간 로드 밸런싱이 해제된 상태에서 네트워크 로드 밸런서와 애플리케이션 로드 밸런서에 대해서만 영역 자동 이동을 구성할 수 있습니다.

관리 리소스

AWS 서비스는 영역 자동 이동을 위해 Route 53 ARC에 리소스를 자동으로 등록합니다. 등록된 리소스는 Route 53 ARC의 관리 리소스입니다.

리소스 이름

Route 53 ARC에 있는 관리 리소스의 이름입니다.

적용 상태

적용 상태는 리소스에 트래픽 전환이 적용되고 있는지를 나타냅니다. 영역 자동 전환을 구성하면 리소스에 활성 트래픽 전환(즉, 연습 실행 영역 전환, 고객 주도 영역 전환 또는 자동 전환)이 두 개 이상 있을 수 있습니다. 하지만 한 번에 한 가지만 적용됩니다. 즉, 한 번에 한 가지만 리소스에 적용됩니다. 상태가 `APPLIED`인 전환은 리소스에 대한 애플리케이션 트래픽이 전환된 소스 가용 영역과 해당 트래픽 전환이 종료되는 시기를 결정합니다.

영역 자동 이동을 위한 데이터 및 컨트롤 플레인

페일오버와 재해 복구를 계획할 때는 페일오버 메커니즘이 얼마나 탄력적인지 생각해 보세요. 재해 시나리오에서 필요할 때 사용할 수 있도록 페일오버 중에 사용하는 메커니즘의 가용성이 높은지 확인하는 것이 좋습니다. 일반적으로 안정성과 내결함성을 극대화하려면 가능하면 언제든지 메커니즘에 데이터 플레인 함수를 사용해야 합니다. 이를 염두에 두고 서비스의 기능이 컨트롤 플레인과 데이터 영역 간에 어떻게 구분되는지, 그리고 서비스의 데이터 영역에서 최상의 신뢰성을 기대할 수 있는 경우를 이해하는 것이 중요합니다.

일반적으로 컨트롤 플레인을 사용하면 서비스의 리소스 생성, 업데이트 및 삭제와 같은 기본 관리 기능을 수행할 수 있습니다. 데이터 영역은 서비스의 핵심 기능을 제공합니다.

데이터 플레인, 컨트롤 플레인, 고가용성 목표를 달성하기 위해 서비스를 AWS 구축하는 방법에 대한 자세한 내용은 Amazon Builders' Library의 가용 영역을 사용한 정적 안정성 문서를 참조하십시오.

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 자동 전환 요금

영역 자동 이동의 경우 고객 애플리케이션에 부정적인 영향을 미칠 수 있는 잠재적 문제가 있다고 AWS 판단되면 지원되는 리소스의 트래픽을 가용 영역 대신 다른 곳으로 AWS 이동시킵니다. 영역 자동 전환을 활성화해도 추가 요금이 부과되지 않습니다.

Amazon Route 53 애플리케이션 복구 컨트롤러에서 사용한 만큼만 비용을 지불하면 됩니다. Route 53 ARC에 대한 자세한 요금 정보와 요금 예제를 보려면 Amazon Route 53 요금을 참조하고 아래로 스크롤하여 Amazon Route 53 애플리케이션 복구 컨트롤러로 이동하십시오.

영역 자동 이동을 구성할 때의 모범 사례

Amazon Route 53 애플리케이션 복구 컨트롤러에서 영역 자동 전환을 활성화할 때는 다음 모범 사례 및 고려 사항을 숙지하십시오.

영역 자동 이동에는 자동 변속과 실제 실행 영역 이동이라는 두 가지 유형의 트래픽 이동이 포함됩니다.

- 자동 전환을 AWS 사용하면 이벤트 발생 시 사용자 대신 애플리케이션 리소스 트래픽을 가용 영역으로 이동시켜 복구 시간을 단축할 수 있습니다.
- 연습을 통해 Route 53 ARC는 사용자를 대신하여 구역 이동을 시작합니다. 영역 이동은 매주 트래픽을 리소스의 가용 영역에서 멀어졌다가 다시 되돌아오게 합니다. 연습 실행을 통해 애플리케이션이 하나의 가용 영역이 손실되더라도 견딜 수 있도록 한 리전의 가용 영역 용량을 충분히 스케일 업했는지 확인할 수 있습니다.

자동 변속 및 연습 실행과 관련하여 염두에 두어야 할 몇 가지 모범 사례와 고려 사항이 있습니다. 리소스에 대한 영역 자동 전환을 활성화하거나 연습 실행을 구성하기 전에 다음 항목을 검토하세요.

주제

- 클라이언트가 엔드포인트에 연결된 상태를 유지하는 시간을 제한하세요.
- 리소스 용량을 미리 확장하고 변화하는 트래픽을 테스트하세요.
- 리소스 유형 및 제한 사항을 숙지하세요.
- 연습 실행을 위한 알람을 지정하십시오.
- 연습 실행 결과 평가

클라이언트가 엔드포인트에 연결된 상태를 유지하는 시간을 제한하세요.

Amazon Route 53 애플리케이션 복구 컨트롤러가 영역 이동 또는 영역 자동 이동을 사용하는 등 장애가 발생하지 않는 곳으로 트래픽을 이동할 때 Route 53 ARC가 애플리케이션 트래픽을 이동하는 데 사용하는 메커니즘은 DNS 업데이트입니다. DNS 업데이트로 인해 모든 새 연결이 손상된 위치에서 멀어집니다. 하지만 기존에 열려 있는 연결이 있는 클라이언트는 클라이언트가 다시 연결될 때까지 손상된 위치에 대해 요청을 계속할 수 있습니다. 빠른 복구를 위해 클라이언트가 엔드포인트에 연결된 상태를 유지하는 시간을 제한하는 것이 좋습니다.

Application Load Balancer를 사용하는 경우 `keepalive` 옵션을 사용하여 연결 지속 시간을 구성할 수 있습니다. 애플리케이션의 복구 시간 목표 (예: 300초) 에 맞도록 `keepalive` 값을 낮추는 것이 좋습니다. `keepalive`시간을 선택할 때 이 값은 일반적으로 지연 시간에 영향을 줄 수 있는 더 자주 다시 연결하는 것과 손상된 AZ 또는 지역에서 모든 클라이언트를 더 빨리 멀어지게 하는 것 사이의 절충점이라는 점을 고려하세요.

Application Load Balancer의 `keepalive` 옵션 설정에 대한 자세한 내용은 애플리케이션 로드 밸런서 사용 설명서의 HTTP 클라이언트 유지 기간을 참조하십시오.

리소스 용량을 미리 스케일링하고 변화하는 트래픽을 테스트하세요.

영역 이동 또는 자동 AWS 이동을 위해 트래픽을 한 가용 영역에서 다른 가용 영역으로 이동할 때는 나머지 가용 영역이 리소스에 대한 증가된 요청 속도를 처리할 수 있는 것이 중요합니다. 이 패턴을 정적 안정성이라고 합니다. 자세한 내용은 Amazon Builder's Library의 Static stability using Availability Zones whitepaper를 참조하세요.

예를 들어 애플리케이션에서 클라이언트에 서비스를 제공하는 데 30개의 인스턴스가 필요한 경우 3개의 가용 영역에 15개의 인스턴스를 프로비저닝하여 총 45개의 인스턴스를 프로비저닝해야 합니다. 이렇게 하면 자동 전환 기능을 사용하거나 연습 실행 중에 트래픽을 하나의 가용 영역에서 다른 가용 영역으로 이동할 때 AWS 두 가용 영역에 걸쳐 나머지 총 30개의 인스턴스로 애플리케이션 클라이언트에 계속 서비스를 제공할AWS 수 있습니다.

Route 53 ARC의 영역 자동 이동 기능을 사용하면 가용 영역 하나가 손실되더라도 정상적으로 작동하도록 리소스가 사전 조정된 애플리케이션이 있는 경우 가용 영역의 AWS 이벤트를 신속하게 복구할 수 있습니다. 리소스에 대한 영역 자동 전환을 활성화하기 전에 AWS 리전내에 구성된 모든 가용 영역의 리소스 용량을 모두 조정하세요. 그런 다음 리소스에 대해 영역 전환을 시작하여 트래픽이 한 가용 영역에서 벗어나도 애플리케이션이 정상적으로 실행되는지 테스트하세요.

영역 전환을 테스트한 후에는 영역 자동 전환을 활성화하고 애플리케이션 리소스에 대한 연습 실행을 구성하세요. 영역 자동 전환을 통한 정기적인 연습 실행은 용량이 여전히 적절하게 조정되고 있는지 지속적으로 확인하는 데 도움이 됩니다. 가용 영역 전체에 충분한 용량이 있으면 자동 전환 중에도 애플리케이션이 중단 없이 클라이언트에 계속 서비스를 제공할 수 있습니다.

리소스에 대한 영역 전환 시작에 대한 자세한 내용은 Amazon Route 53 Application Recovery Controller의 영역 전환 섹션을 참조하세요.

리소스 유형 및 제한 사항을 숙지하세요.

영역 자동 전환은 영역 전환이 지원하는 모든 리소스의 트래픽을 가용 영역 밖으로 이동할 수 있도록 지원합니다. 일반적으로 영역 간 로드 밸런싱이 꺼진 상태의 Application Load Balancer 및 Network Load Balancer가 지원됩니다. 몇 가지 특정 리소스 시나리오에서 영역 자동 전환은 자동 전환을 위해 가용 영역의 트래픽을 이동시키지 않습니다.

예를 들어 가용 영역의 로드 밸런서 대상 그룹에 인스턴스가 없거나 모든 인스턴스가 비정상인 경우 로드 밸런서는 페일 오픈 상태에 있습니다. 이 시나리오에서 로드 밸런서에 대한 자동 전환을 AWS 시작하는 경우 로드 밸런서가 이미 실패 오픈 상태에 있기 때문에 자동 전환으로 인해 로드 밸런서가 사용하는 가용 영역이 변경되지 않습니다. 이는 예상된 동작입니다. 모든 가용 영역이 열리지 않는 AWS 리전 경우 (비정상) 자동 시프트로 인해 한 가용 영역이 비정상 상태가 되어 다른 가용 영역으로 트래픽을 이동할 수는 없습니다.

두 번째 시나리오는 액셀러레이터의 엔드포인트인 Application Load Balancer의 자동 시프트를 AWS 시작하는 경우입니다. AWS Global Accelerator영역 전환과 마찬가지로 글로벌 액셀러레이터에서 액셀러레이터의 엔드포인트인 Application Load Balancer에는 자동 전환이 지원되지 않습니다.

알아야 할 모든 요구 사항 및 예외를 포함하여 지원되는 리소스에 대한 세부 정보를 보려면 영역 전환 및 영역 자동 전환에 지원되는 리소스 섹션을 참조하세요.

연습 실행을 위한 경보를 지정하십시오.

영역 자동 변속 기능이 있는 연습 실행에 대해 하나 이상의 알람 (결과 알람) 을 구성합니다. 선택적으로 두 번째 알람인 차단 알람을 구성할 수도 있습니다.

실습용으로 구성한 CloudWatch 경보가 리소스에 맞게 실행된다는 점을 고려할 때는 다음 사항에 유의하세요.

- 필수 결과 경보의 경우 리소스 또는 애플리케이션에 대한 지표에서 트래픽을 가용 영역 밖으로 이동시키는 것이 성능에 부정적인 영향을 미치는 것으로 나타날 때 `ALARM` 상태가 되도록 CloudWatch 경보를 구성하는 것이 좋습니다. 예를 들어, 리소스에 대한 요청 속도의 임계값을 결정한 다음 임계값이 초과되면 `ALARM` 상태가 되도록 경보를 구성할 수 있습니다. AWS 가 연습 실행을 종료하고 `FAILED` 결과를 반환하도록 하는 적절한 경보를 구성하는 것은 사용자의 책임입니다.
- 핵심 성과 지표 (KPI) 를 경보로 구현하도록 권장하는 AWS Well Architected 프레임워크를 따르는 것이 좋습니다. CloudWatch 이렇게 하면 이러한 경보를 사용하여 안전 트리거로 사용할 복합

경보를 생성하여 애플리케이션이 KPI를 놓칠 수 있는 경우 연습 실행이 시작되지 않도록 할 수 있습니다. 경보가 더 이상 ALARM 상태가 아닌 경우, Route 53 ARC는 리소스에 대한 다음 연습 실행이 예약된 시점에 연습 실행을 시작합니다.

- 연습 실행 차단 경보를 구성하는 경우 연습 실행이 시작되지 않도록 표시하는 데 사용하는 특정 지표를 추적하도록 선택할 수 있습니다.
- 경보를 실제로 실행하려면 먼저 Amazon에서 구성해야 하는 각 경보의 Amazon 리소스 이름(ARN) 을 지정합니다. CloudWatch 지정하는 경보는 복합 CloudWatch 경보가 될 수 있으며, 이를 통해 경보가 특정 상태로 전환되도록 트리거할 수 있는 애플리케이션 및 리소스에 대한 여러 지표와 검사를 포함할 수 있습니다. ALARM 자세한 내용은 Amazon CloudWatch 사용 설명서의 알람 결합을 참조하십시오.
- 연습용으로 지정하는 CloudWatch 경보가 연습 실행을 구성하는 대상 리소스와 동일한 지역에 있는지 확인하십시오.

연습 실행의 결과를 평가하세요.

Route 53 ARC는 각 연습 실행의 결과를 보고합니다. 연습을 실행한 후 결과를 평가하고 조치가 필요한지 결정하십시오. 예를 들어 용량을 확장하거나 알람 구성을 조정해야 할 수 있습니다.

가능한 연습 실행 결과는 다음과 같습니다.

- 성공: 연습 실행 중에 결과 경보가 ALARM 상태에 들어가지 않았고, 연습 실행이 전체 30분의 테스트 기간을 완료했습니다.
- 실패: 연습 실행 중에 결과 경보가 ALARM 상태에 들어갔습니다.
- 중단됨: 결과 경보가 ALARM 상태가 아닌 이유로 연습 실행이 종료되었습니다. 연습 실행은 다음과 같이 여러 가지 이유로 중단될 수 있습니다.
  - 에서 자동 변속이 AWS AWS 리전 시작되었거나 해당 지역에 알람 상태가 발생하여 연습 실행이 종료되었습니다.
  - 리소스에 대한 연습 실행 구성이 삭제되어 연습 실행이 종료되었습니다.
  - 연습 실행 영역 전환이 트래픽을 전환시키던 소스 가용 영역의 리소스에 대해 고객 주도 영역 전환이 시작되어 연습 실행이 종료되었습니다.
  - 연습 실행 구성에 지정된 CloudWatch 경보에 더 이상 액세스할 수 없어 연습 실행이 종료되었습니다.
  - 연습 실행에 지정된 차단 경보가 ALARM 상태에 들어갔기 때문에 연습 실행이 종료되었습니다.
  - 알 수 없는 이유로 연습 실행이 종료되었습니다.
- 보류 중: 연습 실행이 활성화되었습니다(진행 중). 아직 반환할 결과가 없습니다.

영역 자동 전환 API 작업

다음 표에는 영역 자동 전환과 함께 사용할 수 있는 Route 53 ARC API 작업이 나와 있습니다. 에서 영역 자동 이동 API 작업을 사용하는 예는 을 AWS CLI참조하십시오.

AWS Command Line Interface에서 일반적인 영역 자동 전환 API 작업을 사용하는 방법에 대한 예는 영역 AWS CLI 오토시프트와 함께 사용하는 예 섹션을 참조하세요.

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
연습 실행 구성 생성	영역 자동 전환 활성화 또는 비활성화 섹션 참조	을 참조하십시오. CreatePracticeRunConfiguration
연습 실행 구성 삭제	연습 실행 구성 설정, 편집 또는 삭제 섹션 참조	참조 DeletePracticeRunConfiguration
자동 전환 나열	Amazon Route 53 Application Recovery Controller의 영역 자동 전환 섹션 참조	참조 ListAutoshifts
영역 자동 전환을 위한 리소스 나열	영역 전환 및 영역 자동 전환에 지원되는 리소스 섹션 참조	ListManaged리소스 참조
영역 자동 전환을 위한 리소스 가져오기	영역 전환 및 영역 자동 전환에 지원되는 리소스 섹션 참조	GetManaged리소스 참조
연습 실행 구성 편집	연습 실행 구성 설정, 편집 또는 삭제 섹션 참조	참조 UpdatePracticeRunConfiguration
영역 자동 전환 활성화 또는 비활성화	영역 자동 전환 활성화 또는 비활성화 섹션 참조	참조 UpdateZonalAutoshiftConfiguration

영역 AWS CLI 오토시프트와 함께 사용하는 예

이 단원에서는 Amazon Route 53 애플리케이션 복구 컨트롤러에서 API 작업을 AWS Command Line Interface 사용하여 영역 자동 이동 기능을 활용하는 간단한 애플리케이션 예제를 살펴봅니다. 이 예제는 CLI를 사용하여 영역 자동 이동 작업을 수행하는 방법에 대한 기본적인 이해를 돕기 위한 것입니다.

구역 자동 변속은 Route 53 ARC의 기능입니다. 영역 자동 AWS 이동을 사용하면 이벤트 중에 지원되는 애플리케이션 리소스 트래픽을 가용 영역에서 대신 이동시켜 복구 시간을 단축할 수 있습니다. 영역 자동 전환에는 자동 전환이 애플리케이션에 안전한지 지속적으로 확인할 수 있도록 트래픽을 가용 영역 밖으로 이동시키는 연습 실행도 포함됩니다.

현재 영역 자동 전환은 영역 간 로드 밸런싱이 꺼진 상태의 Network Load Balancer 및 Application Load Balancer를 지원합니다.

자세한 정보는 영역 전환 및 영역 자동 전환에 지원되는 리소스을 참조하세요.

이 섹션에서는 영역 자동 전환을 시작하고 사용하는 방법을 설명하는 다음 예를 제공합니다.

- 리소스에 대한 연습 실행 구성을 생성합니다.
- 리소스의 자동 전환을 활성화 및 비활성화합니다.
- 연습 실행으로 시작된 영역 전환을 취소하여 진행 중인 연습 실행을 종료합니다.
- 리소스의 영역 자동 전환 기능을 비활성화하여 진행 중인 자동 전환을 종료합니다.
- 리소스의 연습 실행 구성을 편집하여 지정된 경보나 차단 날짜 또는 기간을 변경합니다.
- 리소스에 대한 연습 실행 구성을 삭제합니다.

사용에 대한 자세한 내용은 명령 AWS CLI참조를 참조하십시오.AWS CLI 영역 자동 전환 API 작업 목록 및 자세한 정보 링크는 영역 자동 전환 API 작업 섹션을 참조하세요.

연습 실행 구성 생성

리소스에 대한 영역 자동 전환을 활성화하려면 먼저 리소스에 대한 연습 실행 구성을 생성하여 필요한 연습 실행에 대한 옵션을 선택해야 합니다. CLI에서 `create-practice-run-configuration` 명령을 사용하여 리소스에 대한 연습 실행 구성을 생성합니다.

리소스에 대한 연습 실행 구성을 생성할 때는 다음 사항을 참고하세요.

- 현재 지원되는 유일한 경보 유형은 `CLOUDWATCH`입니다.
- 리소스가 배포된 AWS 리전 것과 동일한 경보를 사용해야 합니다.
- 결과 경보 지정은 필수 사항입니다. 차단 경보 지정은 선택 사항입니다.
- 차단 날짜 또는 차단 기간 지정은 선택 사항입니다.

CLI에서 `create-practice-run-configuration` 명령을 사용하여 연습 실행 구성을 생성합니다.

예를 들어 리소스에 대한 연습 실행 구성을 생성하려면 다음과 같은 명령을 사용하세요.

```
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"
       ]
}
```

자동 전환 활성화 또는 비활성화

CLI로 영역 자동 전환 상태를 업데이트하여 리소스의 자동 전환을 활성화하거나 비활성화합니다. 영역 자동 전환 상태를 변경하려면 `update-zonal-autoshift-configuration` 명령을 사용합니다.

예를 들어 리소스에 대한 자동 전환을 활성화하려면 다음과 같은 명령을 사용합니다.

```
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"
}
```

진행 중인 자동 전환 취소

리소스에 대해 진행 중인 자동 전환을 취소하려면 영역 자동 전환 기능을 비활성화합니다. 이는 일반적으로 영역 자동 전환을 비활성화할 때 사용하는 명령과 동일하므로 진행 중인 자동 전환을 취소하기 위해 영역 자동 전환을 비활성화해도 리소스는 향후 자동 전환의 영향을 받지 않습니다. 언제든지 영역 자동 전환을 업데이트하여 다시 활성화할 수 있습니다.

참고로 리소스의 연습 실행 구성을 삭제하지 않고도 리소스의 영역 자동 전환을 비활성화할 수 있습니다.

CLI를 사용하여 자동 전환을 취소하려면 `update-zonal-autoshift-configuration` 명령을 사용하여 영역 자동 전환을 비활성화합니다. 예를 들어 리소스에 대한 자동 전환을 종료하려면 다음과 같은 명령을 사용합니다.

```
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"
}
```

진행 중인 연습 실행 취소

CLI를 사용하여 연습 실행이 리소스에 시작한 영역 전환을 취소함으로써 진행 중인 연습 실행을 취소할 수 있습니다. 연습 실행을 취소하려면 `cancel-zonal-shift` 명령을 사용합니다.

예를 들어 리소스에 대한 연습 실행을 취소하려면 다음과 같은 명령을 사용하세요.

```
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"
}
```

연습 실행 구성 편집

CLI로 리소스의 연습 실행 구성을 편집하여 다른 구성 옵션으로 업데이트할 수 있습니다. 예를 들면 연습 실행에 대한 경보를 변경하거나 Route 53 ARC가 연습 실행을 시작하지 않으면 차단 날짜 또는 차단 기간을 업데이트할 수 있습니다. 연습 실행 구성을 편집하려면 `update-practice-run-configuration` 명령을 사용합니다.

리소스에 대한 연습 실행 구성을 편집할 때는 다음 사항을 참고하세요.

- 현재 지원되는 유일한 경보 유형은 `CLOUDWATCH`입니다.
- 리소스가 배포된 AWS 리전 것과 동일한 경보를 사용해야 합니다.
- 결과 경보 지정은 필수 사항입니다. 차단 경보 지정은 선택 사항입니다.
- 차단 날짜 또는 차단 기간 지정은 선택 사항입니다.
- 지정한 차단 날짜 또는 차단 기간은 기존 값을 대체합니다.

예를 들어 리소스의 연습 실행 구성을 편집하여 새 차단 날짜를 지정하려면 다음과 같은 명령을 사용하세요.

```
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"
       ]
}
```

연습 실행 구성 삭제

리소스에 대한 연습 실행 구성을 삭제할 수 있지만 먼저 리소스에 대한 영역 자동 전환을 비활성화해야 합니다. 영역 자동 전환을 활성화하려면 리소스에 연습 실행 구성이 있어야 합니다. 정기적인 연습 실행을 통해 가용 영역 하나가 없어도 애플리케이션이 정상적으로 실행되는지 확인할 수 있습니다.

CLI를 사용하여 연습 실행 구성을 삭제하려면 먼저 `update-zonal-autoshift` 명령을 사용하여 필요한 경우 영역 자동 전환을 비활성화합니다. 그런 다음 연습 실행 구성을 삭제하려면 `delete-practice-run-configuration` 명령을 사용합니다.

먼저 다음과 같은 명령을 사용하여 리소스의 영역 자동 전환을 비활성화합니다.

```
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"
}
```

그런 다음 연습 실행 구성을 삭제하려면 다음과 같은 명령을 사용합니다.

```
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"
}
```

영역 자동 전환 활성화 및 사용

이 섹션에서는 영역 자동 이동을 활성화 및 비활성화하고, 연습 실행을 구성하고, 진행 중인 연습 실행을 취소하는 등 Amazon Route 53 애플리케이션 복구 컨트롤러에서 영역 자동 이동을 사용하는 절차를 제공합니다.

영역 자동 전환 활성화 또는 비활성화

이 섹션의 단계에서는 Amazon Route 53 Application Recovery Controller 콘솔에서 영역 자동 전환을 활성화 또는 비활성화하는 방법을 설명합니다. 프로그래밍 방식으로 영역 자동 전환 작업을 수행하려면 Zonal Shift and Zonal Autoshift API Reference Guide를 참조하세요

영역 자동 전환이 활성화되면 복구 시간을 줄이는 AWS 데 도움이 되도록 이벤트 발생 시 사용자 대신 애플리케이션 리소스 트래픽을 가용 영역에서 이동할 수 있는 권한을 부여합니다.

영역 자동 전환을 활성화하거나 비활성화하는 방법

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 다중 AZ에서 영역 자동 전환을 선택합니다.
3. 리소스 영역 자동 전환 구성에서 리소스를 선택합니다.
4. 작업 메뉴에서 영역 자동 전환 활성화 또는 영역 자동 전환 비활성화를 선택한 다음, 단계에 따라 업데이트를 완료합니다.

리소스에 연습 실행 구성이 없는 경우 영역 자동 전환 활성화를 사용할 수 없습니다. 연습 실행 구성을 구성하고 영역 자동 전환을 활성화하려면 영역 자동 전환 구성을 선택하세요.

연습 실행 구성 설정, 편집 또는 삭제

이 섹션의 단계에서는 Amazon Route 53 Application Recovery Controller 콘솔에서 연습 실행 구성을 편집 또는 삭제하는 방법을 설명합니다. 프로그래밍 방식으로 연습 실행 구성 변경을 비롯한 영역 자동 전환 작업을 수행하려면 Zonal Shift and Zonal Autoshift API Reference Guide를 참조하세요

콘솔에서 연습 실행 구성을 삭제하면 영역 자동 전환이 비활성화됩니다. API 작업을 사용하여 연습 실행 구성을 삭제하려면 먼저 영역 자동 전환을 비활성화해야 합니다. 영역 자동 전환을 활성화하지 않고도 연습 실행을 구성할 수 있습니다. 하지만 리소스에 대해 영역 자동 전환을 활성화하려면 해당 리소스에 연습 실행을 구성해야 합니다.

연습 실행을 구성하는 방법

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 다중 AZ에서 영역 자동 전환을 선택합니다.
3. 영역 자동 전환 구성을 선택합니다.
4. 영역 자동 전환을 구성할 리소스를 선택합니다.
5. 이벤트 발생 시 리소스에 대한 자동 AWS 이동을 시작하지 않으려면 영역 자동 이동을 비활성화하도록 선택하십시오. AWS 원하는 경우 자동 전환을 활성화하지 않고도 마법사를 사용하여 연습 실행 구성을 계속 구성할 수 있습니다.
6. 리소스의 연습 실행 옵션을 선택합니다. 경보의 경우 다음을 수행할 수 있습니다.
   - (필수 사항) 이 리소스의 연습 실행을 모니터링할 결과 경보를 지정합니다.
   - (선택 사항) 이 리소스의 연습 실행에 대한 차단 경보를 지정합니다.

자세한 내용은 영역 자동 이동을 구성할 때의 모범 사례의 연습 실행에 지정하는 경보 섹션을 참조하세요.

7. 선택적으로 차단 날짜와 차단 기간을 지정할 수 있습니다. Route 53 ARC가 이 리소스에 대한 연습 실행을 시작하지 못하도록 하려면 날짜 또는 기간(일 및 시간)을 선택하세요. 모든 날짜와 시간은 UTC 기준입니다.
8. 확인 메모를 읽었음을 확인하는 확인란을 선택합니다.
9. 생성을 선택합니다.

연습 실행 구성을 편집하는 방법

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 다중 AZ에서 영역 자동 전환을 선택합니다.
3. 리소스 영역 자동 전환 구성에서 리소스를 선택합니다.
4. 작업 메뉴에서 연습 실행 구성 편집을 선택합니다.
5. 다음 중 하나 이상의 작업을 수행하려면 연습 실행 구성을 변경합니다.
   - 경보의 경우 다음을 수행할 수 있습니다.
     - 차단 경보의 경우 경보를 추가하거나, 삭제하거나, 다른 차단 경보를 지정할 수 있습니다.
     - 연습 실행을 모니터링하는 결과 경보의 경우 사용할 다른 CloudWatch 경보를 지정할 수 있습니다. 결과 경보는 필수이므로 결과 경보를 삭제할 수 없습니다.
   - 차단 날짜 및 차단 기간의 경우 새 날짜 또는 요일과 시간을 추가하거나 기존 날짜 또는 요일과 시간을 제거하거나 업데이트할 수 있습니다. 모든 날짜와 시간은 UTC 기준입니다.
6. 저장을 선택합니다.

연습 실행 구성을 삭제하는 방법

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 다중 AZ에서 영역 자동 전환을 선택합니다.
3. 리소스 영역 자동 전환 구성에서 리소스를 선택합니다.
4. 작업 메뉴에서 연습 실행 구성 삭제를 선택합니다.

5. 확인 모달 대화 상자에 `Delete`를 입력한 다음 삭제를 선택합니다.

   콘솔에서 연습 실행 구성을 삭제하면 해당 리소스의 영역 자동 전환도 비활성화된다는 점에 유의하세요. 영역 자동 전환을 사용하려면 리소스에 대한 연습 실행을 구성해야 합니다.

연습 실행 영역 전환 취소

이 섹션의 단계에서는 Amazon Route 53 Application Recovery Controller 콘솔에서 영역 전환을 취소하는 방법을 설명합니다. 프로그래밍 방식으로 영역 전환 및 영역 자동 전환 작업을 수행하려면 Zonal Shift and Zonal Autoshift API Reference Guide를 참조하세요

직접 시작한 영역 이동을 취소할 수 있습니다. 영역 자동 이동을 위한 연습 실행을 위해 자원에 대해 AWS 시작하는 영역 이동을 취소할 수도 있습니다.

연습 실행 영역 전환을 취소하는 방법

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 다중 AZ에서 영역 전환을 선택합니다.
3. 취소하려는 영역 전환을 선택한 다음 영역 전환 취소를 선택합니다.
4. 확인 모달 대화 상자에서 확인을 선택합니다.

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 자동 이동에 대한 로깅 및 모니터링

Amazon EventBridge Route 53 애플리케이션 복구 컨트롤러에서 영역 자동 전환을 모니터링하는 데 Amazon을 사용하여 AWS CloudTrail 패턴을 분석하고 문제를 해결할 수 있습니다.

주제

- 를 사용하여 영역 자동 이동 API 호출 로깅 AWS CloudTrail
- Amazon에서 영역 자동 변속 사용하기 EventBridge

를 사용하여 영역 자동 이동 API 호출 로깅 AWS CloudTrail

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 자동 전환은 Route 53 ARC에서 사용자, 역할 또는 서비스가 수행한 작업에 대한 기록을 제공하는 AWS 서비스와 통합되어 있습니다. AWS

CloudTrail CloudTrail 영역 이동에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Route 53 ARC 콘솔에서의 통화와 영역 이동을 위한 Route 53 ARC API 작업에 대한 코드 호출이 포함됩니다.

트레일을 생성하면 영역 이동 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다.

에서 수집한 CloudTrail 정보를 사용하여 영역 이동을 위해 Route 53 ARC에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

구역 자동 변속 정보: CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. 영역 자동 이동을 위해 Route 53 ARC에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. AWS 계정자세한 내용은 CloudTrail 이벤트 기록 작업을 참조하십시오.

Route 53 ARC의 구역 자동 변속 이벤트를 포함하여 내 이벤트의 진행 중인 기록을 보려면 트레일을 생성하십시오 AWS 계정. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Route 53 ARC 작업은 Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 가이드에 의해 CloudTrail 기록되고 문서화되어 있습니다. 예를 들어, `StartZonalShift` 및 `ListManagedResources` 작업에 대한 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail UserIdentity 요소를 참조하십시오.

이벤트 기록에서 Route 53 ARC 이벤트 확인하기

CloudTrail 이벤트 기록에서 최근 이벤트를 볼 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록 작업을 참조하십시오.

영역 자동 변속 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 영역 자동 이동 `ListManagedResources` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.


```
{
      "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"
      }
    }
```

Amazon에서 영역 자동 변속 사용하기 EventBridge

EventBridgeAmazon을 사용하면 영역 자동 이동 리소스를 모니터링하고 다른 서비스를 사용하는 대상 작업을 시작하는 이벤트 기반 규칙을 설정할 수 있습니다. AWS 예를 들어 영역 자동 이동을 위한 연습 실행이 시작될 때 Amazon SNS 주제에 신호를 보내 이메일 알림을 보내는 규칙을 설정할 수 있습니다.

Amazon에서 규칙을 EventBridge 생성하여 영역 자동 이동을 실행할 수 있습니다. 영역 자동 이동 이벤트 이벤트는 연습 실행 자동 이동에 대한 상태 정보 (예: 연습 실행이 진행 중인 경우) 를 지정합니다.

관심 있는 특정 영역 자동 이동 이벤트를 캡처하려면 이벤트를 감지하는 데 사용할 수 있는 이벤트별 패턴을 정의하십시오. EventBridge 이벤트 패턴은 일치하는 이벤트와 동일한 구조를 갖습니다. 패턴은 일치시키려는 필드를 인용하고 찾고 있는 값을 제공합니다.

이벤트는 최선의 작업을 기반으로 발생됩니다. 정상적인 운영 EventBridge 환경에서는 Route 53 ARC 에서 거의 실시간으로 전송됩니다. 하지만 이벤트 전달을 지연하거나 방해하는 상황이 발생할 수 있습니다.

EventBridge 규칙이 이벤트 패턴과 함께 작동하는 방식에 대한 자세한 내용은 의 이벤트 및 이벤트 패턴을 참조하십시오 EventBridge.

다음을 사용하여 영역 자동 이동 리소스를 모니터링하십시오. EventBridge

를 사용하면 Route 53 ARC가 리소스에 대한 이벤트를 내보낼 때 취할 조치를 정의하는 규칙을 생성할 수 있습니다. EventBridge 예를 들어 영역 자동 이동을 위한 연습 실행이 시작될 때 이메일 메시지를 보내는 규칙을 생성할 수 있습니다.

이벤트 패턴을 입력하거나 복사하여 콘솔에 붙여넣으려면 EventBridge 콘솔에서 Enter my own 옵션을 사용하는 옵션을 선택합니다. 유용할 수 있는 이벤트 패턴을 결정하는 데 도움이 되도록 이 항목에는 사용할 수 있는 영역 자동 이동 이벤트 일치 패턴과 영역 자동 이동 이벤트의 예가 포함되어 있습니다.

리소스 이벤트에 대한 규칙을 만들려면

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 규칙을 생성하려는 대상, 즉 이벤트를 시청하고 싶은 지역을 선택합니다. AWS 리전
3. Create rule을 선택합니다.
4. 규칙의 이름을 입력하고 선택적으로 설명을 입력합니다.
5. 이벤트 버스의 경우 기본값을 그대로 두세요.
6. 다음을 선택합니다.
7. 이벤트 패턴 빌드 단계에서 이벤트 소스의 경우 기본값인 AWS 이벤트를 그대로 두세요.
8. 샘플 이벤트에서 직접 입력을 선택합니다.
9. 샘플 이벤트에 이벤트 패턴을 입력하거나 복사하여 붙여넣습니다.

영역 자동 이동 이벤트 패턴 예시

이벤트 패턴은 일치하는 이벤트와 동일한 구조를 갖습니다. 패턴은 일치시키려는 필드를 인용하고 찾고 있는 값을 제공합니다.

이 섹션의 이벤트 패턴을 복사하여 붙여넣어 영역 자동 이동 EventBridge 작업 및 리소스를 모니터링하는 데 사용할 수 있는 규칙을 만들 수 있습니다.

영역 자동 전환 이벤트에 대한 이벤트 패턴을 생성할 때 `detail-type`에 다음 중 하나를 지정할 수 있습니다.

- `Autoshift In Progress`
- `Autoshift Completed`

- Practice Run Started
- Practice Run Succeeded
- Practice Run Interrupted
- Practice Run Failed

연습 실행이 중단된 경우 중단의 원인에 대한 자세한 내용은 additionalFailureInfo 필드를 참조하세요.

- 연습 실행이 시작된 영역 자동 이동에서 모든 이벤트를 선택합니다. .

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

- 영역 자동 변속에서 연습 실행이 실패한 모든 이벤트를 선택합니다. .

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

영역 자동 이동 이벤트의 예

다음은 영역 자동 이동 동작의 예제 이벤트입니다.

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

대상으로 사용할 CloudWatch 로그 그룹을 지정합니다.

규칙을 만들 때는 EventBridge 규칙과 일치하는 이벤트가 전송되는 대상을 지정해야 합니다. 사용 가능한 대상 EventBridge 목록은 EventBridge 콘솔에서 사용 가능한 대상을 참조하십시오. EventBridge 규칙에 추가할 수 있는 대상 중 하나는 Amazon CloudWatch 로그 그룹입니다. 이 섹션에서는 CloudWatch 로그 그룹을 대상으로 추가하기 위한 요구 사항을 설명하고 규칙을 생성할 때 로그 그룹을 추가하는 절차를 제공합니다.

CloudWatch 로그 그룹을 대상으로 추가하려면 다음 중 하나를 수행할 수 있습니다.

- 새 로그 그룹 생성
- 기존 로그 그룹 선택

규칙을 생성할 때 콘솔을 사용하여 새 로그 그룹을 지정하면 이 EventBridge 자동으로 로그 그룹을 생성합니다. EventBridge 규칙의 대상으로 사용하는 로그 그룹이 로 시작하는지 확인하십시오/aws/events. 기존 로그 그룹을 선택하려는 경우 로 시작하는 로그 그룹만 드롭다운 메뉴에 옵션으로 /aws/events 표시된다는 점에 유의하세요. 자세한 내용은 Amazon CloudWatch 사용 설명서의 새 로그 그룹 생성을 참조하십시오.

콘솔 외부의 CloudWatch 작업을 사용하여 대상으로 사용할 CloudWatch 로그 그룹을 만들거나 사용하는 경우 권한을 올바르게 설정해야 합니다. 콘솔을 사용하여 EventBridge 규칙에 로그 그룹을 추가하면 해당 로그 그룹의 리소스 기반 정책이 자동으로 업데이트됩니다. 그러나 AWS Command Line

Interface 또는 AWS SDK를 사용하여 로그 그룹을 지정하는 경우 로그 그룹에 대한 리소스 기반 정책을 업데이트해야 합니다. 다음 예제 정책은 리소스 기반 정책에서 로그 그룹에 정의해야 하는 권한을 보여줍니다.

```
{
  "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"
}
```

콘솔을 사용하여 로그 그룹에 대한 리소스 기반 정책을 구성할 수는 없습니다. 리소스 기반 정책에 필요한 권한을 추가하려면 API 작업을 사용하십시오. CloudWatch PutResourcePolicy 그런 다음 describe-resource-policiesCLI 명령을 사용하여 정책이 올바르게 적용되었는지 확인할 수 있습니다.

리소스 이벤트에 대한 규칙을 생성하고 CloudWatch 로그 그룹 대상을 지정하려면

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 규칙을 AWS 리전 생성하려는 항목을 선택합니다.
3. 규칙 생성을 선택한 다음 해당 규칙에 대한 정보 (예: 이벤트 패턴 또는 일정 세부 정보) 를 입력합니다.

   Route 53 ARC용 EventBridge 규칙 생성에 대한 자세한 내용은 이 주제 앞부분의 섹션을 참조하십시오.
4. 대상 선택 페이지에서 CloudWatch대상으로 선택합니다.
5. 드롭다운 메뉴에서 CloudWatch 로그 그룹을 선택합니다.

영역 자동 전환을 위한 Identity 및 Access Management

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. AWS IAM 관리자는 누가 Route 53 ARC 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

내용

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 자동 전환이 IAM과 함께 작동하는 방식

Amazon Route 53 애플리케이션 복구 컨트롤러에서 IAM을 사용하여 영역 자동 전환에 대한 액세스를 관리하기 전에 영역 자동 전환과 함께 사용할 수 있는 IAM 기능에 대해 알아보십시오.

Amazon Route 53 애플리케이션 복구 컨트롤러에서 영역 자동 전환과 함께 사용할 수 있는 IAM 기능

IAM 특성	영역 자동 이동 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 보안 인증	예

IAM 특성	영역 자동 이동 지원
보안 주체 권한	예
서비스 역할	아니요
서비스 링크 역할	예

AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 개괄적으로 파악하려면 IAM 사용 설명서의 IAM과 연동되는AWS 서비스를 참조하십시오.

Route 53 ARC의 자격 증명 기반 정책

ID 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Route 53 ARC 자격 증명 기반 정책의 예를 보려면 Amazon Route 53 애플리케이션 복구 컨트롤러의 ID 기반 정책 예제 섹션을 참조하세요.

Route 53 ARC 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다.

Route 53 ARC의 정책 작업

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

영역 자동 이동을 위한 Route 53 ARC 작업 목록을 보려면 서비스 권한 부여 참조의 Amazon Route 53 영역 이동에서 정의한 작업을 참조하십시오.

영역 자동 이동을 위한 Route 53 ARC의 정책 조치는 조치 전에 다음 접두사를 사용합니다.

```
arc-zonal-shift
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다. 예를 들면 다음과 같습니다.

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

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `Describe`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

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

영역 자동 이동에 대한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. 영역 자동 전환에 대한 ID 기반 정책 예제

Route 53 ARC의 구역 자동 이동에 대한 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

리소스 유형 및 해당 ARN 목록과 각 리소스의 ARN으로 지정할 수 있는 작업을 보려면 서비스 권한 부여 참조의 다음 항목을 참조하십시오.

- 아마존 Route 53에서 정의한 작업 - 영역 이동

조건 키와 함께 사용할 수 있는 작업 및 리소스를 보려면 서비스 권한 부여 참조의 다음 항목을 참조하십시오.

- Amazon Route 53에서 정의한 조건 키 - 영역 이동

영역 자동 이동에 대한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. 영역 자동 전환에 대한 ID 기반 정책 예제

Route 53 ARC의 영역 자동 이동을 위한 정책 조건 키

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition요소를 지정하거나 단일 Condition요소에서 여러 키를 지정하는 경우 AWS 는 논리적 AND태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

영역 자동 이동을 위한 Route 53 ARC 조건 키 목록을 보려면 서비스 권한 부여 참조의 다음 항목을 참조하십시오.

- Amazon Route 53 영역 전환에 사용되는 조건 키

조건 키와 함께 사용할 수 있는 작업 및 리소스를 보려면 서비스 권한 부여 참조에서 다음 항목을 참조하세요.

- Amazon Route 53 영역 전환에 의해 정의된 작업업

영역 자동 이동에 대한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. 영역 자동 전환에 대한 ID 기반 정책 예제

Route 53 ARC의 액세스 제어 목록(ACL)

ACL 지원	아니요

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Route 53 ARC과 함께하는 ABAC(속성 기반 액세스 제어)

ABAC(정책 내 태그) 지원	부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Route 53 ARC의 구역 자동 변속에는 ABAC에 대한 다음과 같은 부분 지원이 포함됩니다.

- 영역 자동 이동은 영역 이동을 위해 Route 53 ARC에 등록된 관리 리소스에 대해 ABAC를 지원합니다. Network Load Balancer용 ABAC 및 Application Load Balancer에서 관리되는 리소스에 대한 자세한 내용은 Elastic Load Balancing 사용 설명서에서 Elastic Load Balancer를 사용하는 ABC를 참조하세요.

Route 53 ARC에서 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 일부 기능이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

Route 53 ARC의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원	예

IAM 개체 (사용자 또는 역할) 를 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 정책은 보안 주체에게 권한을 부여합니다. 일부 서비스를 사용할 때는 다른 서비스에서 다른 작업을 트리거하는 작업을 수행할 수 있습니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다.

작업에 정책의 종속 작업이 추가로 필요한지 알아보려면 서비스 권한 부여 참조의 다음 주제를 참조하십시오.

- Amazon Route 53 영역 전환

Route 53 ARC의 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조합니다.

Route 53 ARC의 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Route 53 ARC 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 Route 53 ARC에서 영역 자동 이동을 위한 서비스 연결 역할 사용 섹션을 참조하세요.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스 단원을 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

영역 자동 전환에 대한 ID 기반 정책 예제

기본적으로 사용자 및 역할에는 Route 53 ARC 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 API를 사용하여 작업을 수행할 수 없습니다. AWS 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 비롯하여 Route 53 ARC에 의해 정의되는 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 Amazon Route 53 Application Recovery Controller에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- 예: 영역 자동 전환 콘솔 액세스
- 예제: Route 53 ARC API 작업

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Route 53 ARC 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있

는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.

- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

예: 영역 자동 전환 콘솔 액세스

Amazon Route 53 Application Recovery Controller 콘솔에 액세스하려면 최소한의 권한 세트가 있어야 합니다. 이러한 권한을 통해 내 Route 53 ARC 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

일부 작업을 수행하려면 사용자에게 Route 53 ARC에서 영역 자동 전환과 관련된 서비스 연결 역할을 생성할 권한이 있어야 합니다. 자세한 내용은 Route 53 ARC에서 영역 자동 이동을 위한 서비스 연결 역할 사용 섹션을 참조하세요.

사용자에게 에서 영역 자동 전환을 사용할 수 있는 전체 액세스 권한을 부여하려면 다음과 같은 정책을 사용자에게 연결하십시오. AWS Management Console

```
{
    "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": "*"
        }
    ]
}
```

예제: Route 53 ARC API 작업

정책을 사용하여 사용자가 영역 자동 전환용 Route 53 ARC API 작업을 사용하여 영역 자동 전환을 구성하여 애플리케이션 리소스 트래픽을 사용자 대신 가용 영역의 정상 AZ로 이동시켜 이벤트 발생 AWS 시 복구 시간을 줄일 수 있도록 할 수 있습니다. AWS 리전이러한 권한을 제공하려면 아래 설명과 같이 사용자가 작업해야 하는 API 작업에 해당하는 정책을 연결하십시오.

일부 작업을 수행하려면 사용자에게 Route 53 ARC와 연결된 서비스 연결 역할에 대한 권한이 있어야 합니다. 서비스 연결 역할을 생성하는 데 필요한 권한은 다음 예제 정책에 포함되어 있습니다. 자세한 내용은 Route 53 ARC에서 영역 자동 이동을 위한 서비스 연결 역할 사용 섹션을 참조하세요.

영역 자동 이동을 위한 API 작업을 사용하려면 다음과 같은 정책을 사용자에게 연결하세요.

```
{
    "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" : "*"
        }
    ]
}
```

Route 53 ARC에서 영역 자동 이동을 위한 서비스 연결 역할 사용

Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 자동 전환은 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 서비스(이 경우에는 Route 53 ARC)에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Route 53 ARC에 의해 사전 정의되며, 서비스가 특정 목적을 위해 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할은 Route 53 ARC를 더 쉽게 설정할 수 있습니다. Route 53 ARC는 서비스 연결 역할에 대한 권한을 정의하며, 달리 정의되지 않는 한 Route 53 ARC만 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스 액세스 권한을 실수로 제거할 수 없으므로 Route 53 ARC 영역 자동 이동 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 표시된 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

에 대한 서비스 연결 역할 권한 AWSServiceRoleForZonalAutoshiftPracticeRun

Route 53 ARC는 이름이 지정된 서비스 연결 역할을 AWSServiceRoleForZonalAutoshiftPracticeRun사용하여 다음을 수행합니다.

- 연습 실행을 위해 고객이 제공한 Amazon CloudWatch 알람 및 고객 AWS Health Dashboard 이벤트를 모니터링합니다.
- 연습 실행 관리(영역 전환 연습)

이 섹션에서는 서비스 연결 역할에 대한 권한과 역할 생성, 편집 및 삭제에 대한 정보를 설명합니다.

에 대한 서비스 연결 역할 권한 AWSServiceRoleForZonalAutoshiftPracticeRun

서비스 연결 역할은 관리형 정책 `AWSZonalAutoshiftPracticeRunSLRPolicy`를 사용합니다.

AWSServiceRoleForZonalAutoshiftPracticeRun서비스 연결 역할은 다음 서비스가 역할을 맡을 것으로 신뢰합니다.

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

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSZonalAutoshiftPracticeRunSLRPolicy.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Route 53 ARC에 대한 AWSServiceRoleForZonalAutoshiftPracticeRun서비스 연결 역할 생성

AWSServiceRoleForZonalAutoshiftPracticeRun서비스 연결 역할을 수동으로 생성할 필요는 없습니다. AWS Management Console AWS CLI, 또는 AWS SDK에서 첫 번째 연습 실행 구성을 생성하면 Route 53 ARC가 서비스 연결 역할을 자동으로 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 첫 번째 연습 실행 구성을 생성하면 Route 53 ARC가 대신해서 서비스 연결 역할을 다시 생성합니다.

Route AWSServiceRoleForZonalAutoshiftPracticeRun53 ARC의 서비스 연결 역할 편집

Route 53 ARC에서는 AWSServiceRoleForZonalAutoshiftPracticeRun서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다른 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Route AWSServiceRoleForZonalAutoshiftPracticeRun53 ARC의 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

자동 전환을 비활성화한 후에는 서비스 연결 역할을 삭제할 수 있습니다. AWSServiceRoleForZonalAutoshiftPracticeRun 자동 전환 기능에 대한 자세한 내용은 Amazon Route 53 Application Recovery Controller의 영역 전환 섹션을 참조하세요.

> **Note**
>
> 리소스를 삭제하려 할 때 Route 53 ARC 서비스가 역할을 사용 중이면 서비스 역할 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 역할 삭제를 다시 시도하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 서비스 연결 역할을 삭제합니다. AWSServiceRoleForZonalAutoshiftPracticeRun 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

영역 자동 이동을 위한 Route 53 ARC 서비스 연결 역할 업데이트

Route 53 ARC 서비스 연결 역할의 AWS 관리형 정책 업데이트는 Route 53 ARC의AWS 관리형 정책 업데이트 표를 참조하십시오. Route 53 ARC 문서 기록 페이지에서 자동 RSS 알림을 구독할 수도 있습니다.

AWS Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 자동 이동에 대한 관리형 정책

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSZonalAutoshiftPracticeRunSLRPolicy

`AWSZonalAutoshiftPracticeRunSLRPolicy`를 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Amazon Route 53 애플리케이션 복구 컨트롤러가 영역 자동 전환을 위해 다음을 수행할 수 있도록 하는 서비스 연결 역할에 연결됩니다.

- 연습 실행을 위해 고객이 제공한 Amazon CloudWatch 알람 및 고객 AWS Health Dashboard 이벤트를 모니터링합니다.
- 연습 실행 관리(영역 전환 연습)

자세한 정보는 Route 53 ARC에서 영역 자동 이동을 위한 서비스 연결 역할 사용을 참조하세요.

영역 자동 이동에 대한 AWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Route 53 ARC의 영역 자동 이동에 대한 AWS 관리형 정책 업데이트에 대한 자세한 내용은 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 AWS 관리형 정책 업데이트 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 Route 53 ARC 문서 기록 페이지에서 RSS 피드를 구독합니다.

Amazon Route 53 애플리케이션 복구 컨트롤러에서 라우팅 제어를 사용하여 다중 지역 애플리케이션을 복구할 수 있습니다.

이 섹션에서는 애플리케이션을 여러 곳에 배포한 경우 Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어 기능을 사용하여 중단을 최소화하고 사용자에게 연속성을 제공하는 방법을 설명합니다. AWS AWS 리전

또한 애플리케이션과 리소스가 복구 준비가 되었는지 여부를 파악하는 데 사용할 수 있는 Route 53 ARC의 기능인 준비 상태 확인에 대해서도 알아볼 수 있습니다.

이 섹션의 항목에서는 라우팅 제어 및 준비 검사 기능, 설정 방법 및 사용 방법에 대해 설명합니다.

주제

Amazon Route 53 Application Recovery Controller의 라우팅 제어

여러 AWS 리전애플리케이션 복제본으로 트래픽을 페일오버하려면 Amazon Route 53의 특정 종류의 상태 확인과 통합된 Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 사용할 수 있습니다. 라우팅 컨트롤은 클라이언트 트래픽을 한 지역 복제본에서 다른 지역 복제본으로 전환할 수 있는 간단한 온-오프 스위치입니다. 트래픽 재라우팅은 Amazon Route 53 DNS 레코드로 설정된 라우팅 제어 상태 확인을 통해 이루어집니다. 예를 들어 각 지역의 애플리케이션 복제본 앞에 있는 도메인 이름과 관련된 DNS 장애 조치 레코드가 여기에 해당합니다.

이 섹션에서는 라우팅 제어의 작동 방식, 라우팅 제어 구성 요소를 설정하는 방법, 이러한 구성 요소를 사용하여 장애 조치를 위해 트래픽을 다시 라우팅하는 방법을 설명합니다.

Route 53 ARC의 라우팅 제어 구성 요소는 클러스터, 제어판, 라우팅 제어, 라우팅 제어 상태 확인입니다. 모든 라우팅 제어는 제어판에 그룹화되어 있습니다. Route 53 ARC가 클러스터용으로 생성하는 기본 제어판에서 이들을 그룹화하거나 사용자 지정 제어판을 생성할 수 있습니다. 제어판 또는 라우팅 제어를 만들려면 먼저 클러스터를 생성해야 합니다. Route 53 ARC의 각 클러스터는 5개의 AWS 리전엔드포인트로 구성된 데이터 영역입니다.

라우팅 제어 및 라우팅 제어 상태 점검을 생성한 후에는 의도하지 않은 복구 자동화의 부작용을 방지하는 데 도움이 되는 라우팅 제어에 대한 안전 규칙을 생성할 수 있습니다. 또는 API 작업 (권장) 을 사용하거나 를 사용하여 개별적으로 또는 일괄적으로 트래픽을 다시 라우팅하도록 라우팅 제어 상태를 업데이트할 수 있습니다. AWS CLI AWS Management Console

이 섹션에서는 라우팅 컨트롤의 작동 방식과 라우팅 컨트롤을 생성하고 이를 사용하여 애플리케이션의 트래픽을 다시 라우팅하는 방법을 설명합니다.

> **Important**
>
> 재해 시나리오에서 애플리케이션의 장애 조치 계획의 일환으로 Route 53 ARC를 사용하여 트래픽을 다시 라우팅하도록 준비하는 방법에 대해 알아보려면 Route 53 ARC에서의 라우팅 제어에 대한 모범 사례 섹션을 참조하세요.

라우팅 제어에 대한 정보

라우팅 제어는 복구 그룹 내 셀의 최상위 리소스(예: Elastic Load Balancing 로드 밸런서)와 관련된 DNS 레코드로 구성된 Amazon Route 53의 상태 확인을 사용하여 트래픽을 리디렉션합니다. 예를 들어 라우팅 제어 상태를 `Off`(한 셀로의 트래픽 흐름 중지)로 업데이트하고 다른 라우팅 제어 상태를 On(다른 셀로의 트래픽 흐름 시작)로 업데이트하여 한 셀에서 다른 셀로 트래픽을 리디렉션할 수 있습니다. 트래픽 흐름을 변경하는 프로세스는 해당 라우팅 제어 상태에 따라 Route 53 ARC가 정상 또는 비정상으로 업데이트한 후 라우팅 제어와 연결된 Route 53 상태 확인입니다.

라우팅 컨트롤은 DNS 엔드포인트가 있는 모든 AWS 서비스에서 장애 조치를 지원합니다. 재해 복구를 위해 또는 애플리케이션의 지연 시간 감소 또는 기타 문제가 감지될 때 트래픽을 장애 조치하도록 라우팅 제어 상태를 업데이트할 수 있습니다.

또한 라우팅 제어를 사용하여 트래픽을 다시 라우팅해도 가용성이 저하되지 않도록 라우팅 제어에 대한 안전 규칙을 구성할 수 있습니다. 자세한 정보는 라우팅 제어를 위한 안전 규칙 만들기 을 참조하세요.

중요한 점은 라우팅 제어 자체가 엔드포인트의 기본 상태를 모니터링하는 상태 확인이 아니라는 점입니다. 예를 들어, Route 53 상태 확인과 달리 라우팅 제어는 응답 시간 또는 TCP 연결 시간을 모니터링하지 않습니다. 라우팅 제어는 상태 확인을 제어하는 간단한 온-오프 스위치입니다. 일반적으로 상태를 변경하여 트래픽을 리디렉션하고 해당 상태 변경으로 인해 트래픽이 전체 애플리케이션 스택의 특정 엔드포인트로 이동하거나 전체 애플리케이션 스택으로의 라우팅이 차단됩니다. 예를 들어 간단한 시나리오에서 라우팅 제어 상태를 On에서 `Off`로 변경하면 DNS 장애 조치 레코드에 연결한 Route 53 상태 확인이 업데이트되어 트래픽이 엔드포인트 외부로 이동합니다.

라우팅 제어 사용 방법

트래픽을 다시 라우팅할 수 있도록 라우팅 제어 상태를 업데이트하려면 Route 53 ARC의 클러스터 엔드포인트 중 하나에 연결해야 합니다. 연결하려는 엔드포인트를 사용할 수 없는 경우 다른 클러스터 엔드포인트로 상태를 변경해 보세요. 정기적인 유지 관리 및 업데이트를 위해 클러스터 엔드포인트가 사용 가능 상태와 사용 불가능 상태로 순환되므로 라우팅 제어 상태를 변경하는 프로세스에서는 각 엔드포인트를 번갈아 시도할 수 있도록 준비해야 합니다.

라우팅 제어를 생성할 때는 라우팅 제어 상태 확인을 각 애플리케이션 복제본의 앞에 있는 Route 53 DNS 이름과 연결하도록 DNS 레코드를 구성합니다. 예를 들어 두 리전에 각각 하나씩 있는 두 로드 밸런서의 트래픽 장애 조치를 제어하려면 두 라우팅 제어 상태 확인을 생성하고 이를 두 DNS 레코드(예: 각 로드 밸런서의 도메인 이름과 함께 장애 조치 라우팅 정책이 있는 별칭 레코드)에 연결합니다.

또한 가중치 기반 라우팅 정책이 적용된 DNS 레코드를 통해 Route 53 ARC 라우팅 제어를 Route 53 상태 확인 및 DNS 레코드 세트와 함께 사용하여 더 복잡한 트래픽 장애 조치 시나리오를 설정할 수 있습니다. 자세한 예를 보려면 다음 AWS 블로그 게시물의 사용자 트래픽 장애 조치 섹션을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러를 사용하여 복원력이 뛰어난 애플리케이션 구축, 2부: 다중 지역 스택

라우팅 제어를 AWS 리전 사용하여 장애 조치를 시작하면 트래픽 흐름과 관련된 단계로 인해 트래픽이 지역 밖으로 즉시 이동하지 않을 수 있습니다. 또한 클라이언트 동작 및 연결 재사용에 따라 해당 지역에서 진행 중인 기존 연결이 완료되는 데 시간이 조금 걸릴 수 있습니다. DNS 설정 및 기타 요인에 따라 기존 연결은 단 몇 분 만에 완료될 수도 있고 더 오래 걸릴 수도 있습니다. 자세한 내용은 트래픽 이동이 빠르게 완료되도록 하기를 참조하십시오.

라우팅 제어 사용 방법

Route 53 ARC의 라우팅 제어는 기존 상태 확인을 사용하여 트래픽을 다시 라우팅하는 것보다 몇 가지 이점이 있습니다. 예:

- 라우팅 제어를 사용하면 전체 애플리케이션 스택에 대해 장애 조치를 취할 수 있습니다. 이는 Amazon EC2 인스턴스처럼 리소스 수준 상태 확인을 기반으로 스택의 개별 구성 요소에 대해 장애가 발생하는 것과는 대조적입니다.
- 라우팅 제어를 사용하면 내부 모니터에서 문제가 감지되지 않을 때 트래픽을 이동하여 유지 관리를 수행하거나 장애 복구를 위해 사용할 수 있는 안전하고 간단한 수동 재정의 기능을 사용할 수 있습니다.
- 라우팅 제어를 안전 규칙과 함께 사용하면 장애 조치가 준비되지 않은 대기 인프라로 장애 조치하는 등 완전히 자동화된 상태 확인 기반 자동화에서 발생할 수 있는 일반적인 부작용을 방지할 수 있습니다.

다음은 에서 애플리케이션의 복원력과 가용성을 개선하기 위해 라우팅 제어를 페일오버 전략에 통합하는 예입니다. AWS

여러 지역 간에 여러 개 (일반적으로 3개) 의 중복 AWS 복제본을 실행하여 가용성이 높은 AWS 애플리케이션을 지원할 수 있습니다. 그런 다음 Amazon Route 53 라우팅 제어를 사용하여 적절한 복제본으로 트래픽을 라우팅할 수 있습니다.

예를 들어 하나의 애플리케이션 복제본이 활성 상태이고 애플리케이션 트래픽을 처리하도록 설정하고 다른 애플리케이션 복제본은 대기 복제본이 되도록 설정할 수 있습니다. 활성 복제본에 장애가 발생한 경우 사용자 트래픽을 해당 복제본으로 다시 라우팅하여 애플리케이션의 가용성을 복원할 수 있습니다. 모니터링 및 상태 점검 시스템의 정보를 기반으로 복제본에서 페일오버할지 아니면 복제본으로 페일링할지 결정해야 합니다.

복구 속도를 높이려는 경우 아키텍처에 맞게 선택할 수 있는 또 다른 옵션은 활성-활성 구현입니다. 이 접근 방식을 사용하면 복제본이 동시에 활성화됩니다. 즉, 트래픽을 다른 활성 복제본으로 다시 라우팅하기만 하면 손상된 애플리케이션 복제본으로부터 사용자를 이동시켜 장애를 복구할 수 있습니다.

AWS 라우팅 제어를 위한 지역 가용성

Amazon Route 53 Application Recovery Controller의 리전 지원 및 서비스 엔드포인트에 대한 자세한 내용은 Amazon Web Services 일반 참조의 Amazon Route 53 Application Recovery Controller 엔드포인트 및 할당량을 참조하세요.

> **Note**
>
> Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어는 글로벌 기능입니다. 하지만 Regional Route 53 ARC AWS CLI 명령에서 미국 서부 (오레곤) 지역 (매개변수 지정`--region us-west-2`) 을 지정해야 합니다. 클러스터, 제어판 또는 라우팅 컨트롤과 같은 리소스를 생성할 때입니다.

Route 53 ARC 라우팅 제어는 Route 53 ARC 상태 확인의 상태를 변경하는 켜기/끄기 스위치이며, 이를 DNS 레코드에 연결하여 트래픽을 예를 들어 기본 복제본에서 대기 배포 복제본으로 리디렉션할 수 있습니다.

애플리케이션 장애 또는 지연 문제가 있는 경우 라우팅 제어 상태를 업데이트하여 트래픽을 기본 복제본에서 예를 들어 대기 복제본으로 이동할 수 있습니다. 매우 안정적인 Route 53 ARC 데이터 영역 API 작업을 사용하여 라우팅 제어 쿼리 및 라우팅 제어 상태 업데이트를 수행하면 재해 복구 시나리오 중에

Route 53 ARC를 사용하여 장애 조치를 수행할 수 있습니다. 자세한 정보는 Route 53 ARC API를 사용하여 라우팅 제어 상태 가져오기 및 업데이트(권장)을 참조하세요.

Route 53 ARC는 5개의 중복 리전 엔드포인트 세트인 클러스터에서 라우팅 제어 상태를 유지합니다. Route 53 ARC는 Amazon EC2 플릿에 위치한 클러스터 전체에 라우팅 제어 상태 변경을 전파하여 5개 지역에 걸쳐 쿼럼을 확보합니다. AWS 전파 후 API 및 매우 안정적인 데이터 영역을 사용하여 Route 53 ARC에 라우팅 제어 상태를 쿼리하면 합의 뷰가 반환됩니다.

5개 클러스터 엔드포인트 중 하나와 상호 작용하여 라우팅 제어 상태를 예를 들어 `Off`에서 `On`으로 업데이트할 수 있습니다. 그런 다음 Route 53 ARC는 클러스터의 5개 리전에 업데이트를 전파합니다.

5개 클러스터 엔드포인트 모두의 데이터 일관성은 평균 5초 이내에, 최대 15초 이내에 달성됩니다.

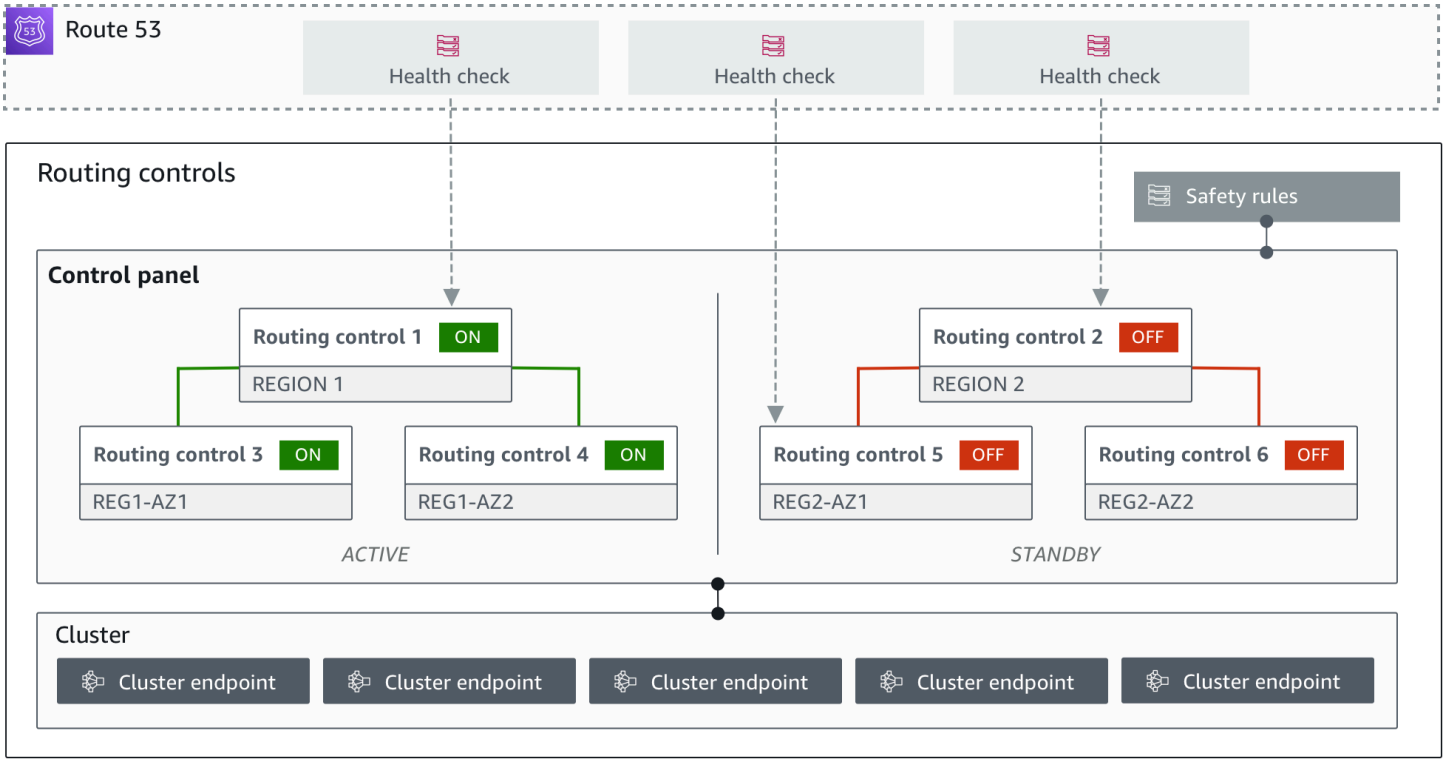
Route 53 ARC는 셀 간에 애플리케이션을 수동으로 장애 조치할 수 있는 데이터 영역을 통해 최상의 신뢰성을 제공합니다. Route 53 ARC는 5개 클러스터 엔드포인트 중 3개 이상이 항상 액세스하여 라우팅 제어 상태 변경을 수행할 수 있도록 합니다. 각 Route 53 ARC 클러스터는 단일 테넌트이므로 액세스 패턴을 느리게 할 수 있는 "시끄러운 인접" 클러스터의 영향을 받지 않습니다.

라우팅 제어 상태를 변경할 때는 실패할 가능성이 매우 낮은 다음 세 가지 기준을 따르게 됩니다.

- 5개 엔드포인트 중 3개 이상을 사용할 수 있으며 쿼럼에 참여합니다.
- 작동하는 IAM 보안 인증 정보가 있고 작동하는 리전 클러스터 엔드포인트에 대해 인증할 수 있습니다.
- Route 53 데이터 영역은 정상입니다(이 데이터 영역은 100% 가용성 SLA를 충족하도록 설계됨).

라우팅 제어 구성 요소

다음 다이어그램은 Route 53 ARC에서 라우팅 제어 기능을 지원하는 구성 요소의 예를 보여줍니다. 여기에 표시된 라우팅 제어(하나의 제어판으로 그룹화)을 사용하면 두 리전 각각의 두 가용 영역에 대한 트래픽을 관리할 수 있습니다. 라우팅 제어 상태를 업데이트하면 Route 53 ARC가 Amazon Route 53의 상태 확인을 변경하여 DNS 트래픽을 다른 셀로 리디렉션합니다. 라우팅 제어를 위해 구성한 안전 규칙은 장애 발생 시나리오 및 기타 의도하지 않은 결과를 방지하는 데 도움이 됩니다.



Route 53 ARC의 라우팅 제어 기능 구성 요소는 다음과 같습니다.

클러스터

클러스터는 라우팅 제어 상태를 업데이트하거나 가져오기 위해 API 직접 호출을 시작하는 5개의 중복 리전 엔드포인트 세트입니다. 클러스터에는 기본 제어판이 포함되며 한 클러스터에서 여러 개의 제어판과 라우팅 제어를 호스팅할 수 있습니다.

라우팅 제어

라우팅 제어는 클러스터에서 호스팅되는 간단한 켜기/끄기 스위치로, 셀에서 들어오고 나가는 클라이언트 트래픽의 라우팅을 제어하는 데 사용합니다. 라우팅 제어를 생성할 때는 Route 53에 Route 53 ARC 상태 확인을 추가합니다. 그러면 Route 53 ARC에서 라우팅 제어 상태를 업데이트할 때 애플리케이션의 DNS 레코드로 구성된 상태 확인을 사용하여 트래픽을 다시 라우팅할 수 있습니다.

라우팅 제어 상태 확인

라우팅 제어는 Route 53의 상태 확인과 통합됩니다. 상태 확인은 각 애플리케이션 복제본의 앞에 있는 DNS 레코드(예: 장애 조치 레코드)와 연결됩니다. 라우팅 제어 상태를 변경하면 Route 53 ARC가 해당 상태 확인을 업데이트하여 트래픽을 리디렉션(예: 대기 복제본으로 장애 조치)합니다.

제어판

제어판은 관련된 라우팅 제어 세트를 그룹화합니다. 여러 라우팅 제어을 하나의 제어판에 연결한 다음 제어판에 대한 안전 규칙을 만들어 트래픽 리디렉션 업데이트가 안전한지 확인할 수 있습니다. 예를 들어 각 가용 영역의 각 로드 밸런서에 대한 라우팅 제어를 구성한 다음 동일한 제어판에서 그룹화할 수 있습니다. 그런 다음, 한 번에 하나 이상의 영역(라우팅 제어로 표시됨)이 활성화되도록 하는 안전 규칙("어설션 규칙")을 추가하여 의도하지 않은 "페일 오픈" 시나리오를 방지할 수 있습니다.

기본 제어판

클러스터를 생성하면 Route 53 ARC가 기본 제어판을 생성합니다. 기본적으로 클러스터에서 생성한 모든 라우팅 제어가 기본 제어판에 추가됩니다. 또는 자체 제어판을 만들어 관련 라우팅 제어를 그룹화할 수도 있습니다.

안전 규칙

안전 규칙은 복구 작업으로 인해 애플리케이션 가용성이 실수로 손상되지 않도록 라우팅 제어에 추가하는 규칙입니다. 예를 들어 전체 "켜기/끄기" 스위치 역할을 하는 라우팅 제어를 생성하는 안전 규칙을 생성하여 다른 라우팅 제어 세트를 활성화하거나 비활성화할 수 있습니다.

엔드포인트(클러스터 엔드포인트)

Route 53 ARC의 각 클러스터에는 라우팅 제어 상태를 설정하고 검색하는 데 사용할 수 있는 5개의 리전 엔드포인트가 있습니다. 엔드포인트에 액세스하는 프로세스에서는 Route 53 ARC가 유지 관리를 위해 엔드포인트를 정기적으로 가동 및 중단한다고 가정해야 하므로, 엔드포인트에 연결할 때까지 각 엔드포인트를 연속해서 시도해야 합니다. 엔드포인트에 액세스하여 라우팅 제어의 현재 상태(켜짐 또는 꺼짐)를 확인하고 라우팅 제어 상태를 변경하여 애플리케이션에 대한 장애 조치를 트리거할 수 있습니다.

라우팅 제어를 위한 데이터 및 컨트롤 플레인

페일오버와 재해 복구를 계획할 때는 페일오버 메커니즘이 얼마나 탄력적인지 생각해 보세요. 재해 시나리오에서 필요할 때 사용할 수 있도록 페일오버 중에 사용하는 메커니즘의 가용성이 높은지 확인하는 것이 좋습니다. 일반적으로 안정성과 내결함성을 극대화하려면 가능하면 언제든지 메커니즘에 데이터 플레인 함수를 사용해야 합니다. 이를 염두에 두고 서비스의 기능이 컨트롤 플레인과 데이터 영역 간에 어떻게 구분되는지, 그리고 서비스의 데이터 영역에서 최상의 신뢰성을 기대할 수 있는 경우를 이해하는 것이 중요합니다.

대부분의 AWS 서비스와 마찬가지로 라우팅 제어 기능에 대한 기능은 컨트롤 플레인 및 데이터 플레인에서 지원됩니다. 둘 다 신뢰성을 위해 구축되었지만 컨트롤 플레인은 데이터 일관성을 위해 최적화되

고 데이터 플레인은 가용성을 위해 최적화됩니다. 데이터 영역은 복원력을 고려하여 설계되었으므로 컨트롤 플레인 사용이 불가능해질 수 있는 운영 중단에도 가용성을 유지할 수 있습니다.

일반적으로 컨트롤 플레인을 사용하면 서비스의 리소스 생성, 업데이트 및 삭제와 같은 기본 관리 기능을 수행할 수 있습니다. 데이터 영역은 서비스의 핵심 기능을 제공합니다. 따라서 가용성이 중요한 경우(예: 가동 중단 중에 트래픽을 대기 복제본으로 다시 라우팅해야 하는 경우) 데이터 영역 작업을 사용하는 것이 좋습니다.

라우팅 제어의 경우 컨트롤 플레인과 데이터 플레인은 다음과 같이 구분됩니다.

- 라우팅 제어를 위한 컨트롤 플레인 API는 미국 서부 (오레곤) 지역 (us-west-2) 에서 지원되는 복구 제어 구성 API입니다. 이러한 API 작업 또는 AWS Management Console 를 사용하여 클러스터, 컨트롤 패널 및 라우팅 컨트롤을 만들거나 삭제하면 애플리케이션의 트래픽을 다시 라우팅해야 할 때 재해 복구 이벤트에 대비할 수 있습니다. 라우팅 제어 구성 컨트롤 플레인은 가용성이 높지 않습니다.
- 라우팅 제어 데이터 플레인은 지리적으로 분리된 5개 지역에 AWS 걸친 전용 클러스터입니다. 각 고객은 라우팅 컨트롤 플레인을 사용하여 하나 이상의 클러스터를 생성합니다. 클러스터는 제어판 및 라우팅 제어를 호스팅합니다. 그런 다음 애플리케이션의 트래픽을 다시 라우팅하려는 경우 라우팅 제어(복구 클러스터) API를 사용하여 라우팅 제어 상태를 가져오고, 나열하고, 업데이트합니다. 라우팅 제어 데이터 영역은 가용성이 높습니다.

라우팅 제어 데이터 플레인은 가용성이 높으므로 이벤트 복구를 위해 페일오버하려는 경우 AWS Command Line Interface 를 사용하여 API를 호출하여 라우팅 제어 상태를 처리하도록 계획하는 것이 좋습니다. 라우팅 제어를 통한 복구 작업을 준비하고 완료할 때의 주요 고려 사항에 대한 자세한 내용은 을 참조하십시오Route 53 ARC에서의 라우팅 제어에 대한 모범 사례.

데이터 플레인, 컨트롤 플레인, 고가용성 목표를 달성하기 위해 서비스를 AWS 구축하는 방법에 대한 자세한 내용은 Amazon Builders' Library의 가용 영역을 사용한 정적 안정성 문서를 참조하십시오.

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 태깅

태그는 리소스를 식별하고 구성하는 데 AWS 사용하는 단어 또는 구문 (메타데이터) 입니다. 각 리소스에 태그를 여러 개 추가할 수 있고, 각 태그는 사용자가 정의한 키와 값을 포함할 수 있습니다. 예를 들어, 키는 환경이고 값은 생산일 수 있습니다. 추가하는 태그에 따라 리소스를 검색하고 필터링할 수 있습니다.

Route 53 ARC의 라우팅 제어에서 다음 리소스를 태그할 수 있습니다.

- 클러스터

- 제어판
- 안전 규칙

Route 53 ARC에서의 태그 지정은 API를 통해서만 사용할 수 있습니다(예: AWS CLI사용).

다음은 를 사용하여 라우팅 제어에서 태그를 지정하는 예입니다. 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
```

자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러용 복구 제어 구성 API 참조 안내서를 참조하십시오 TagResource.

Route 53 ARC에서의 라우팅 제어 요금

Amazon Route 53 Application Recovery Controller를 사용하면 서비스에서 사용하도록 구성한 만큼만 비용을 지불하면 됩니다. Route 53 ARC의 라우팅 제어의 경우 생성한 클러스터당 시간당 비용을 지불합니다. 각 클러스터는 애플리케이션 장애 조치를 트리거하는 데 사용하는 여러 라우팅 제어를 호스팅할 수 있습니다.

비용을 관리하고 효율성을 개선하기 위해 클러스터에 대한 계정 간 공유를 설정하여 하나의 클러스터를 여러 AWS 계정과 공유할 수 있습니다. 자세한 정보는 Route 53 ARC의 클러스터에 대한 크로스 계정 지원을 참조하세요.

Route 53 ARC에 대한 자세한 요금 정보와 요금 예제를 보려면 Amazon Route 53 애플리케이션 복구 컨트롤러 요금을 참조하고 Amazon Route 53 애플리케이션 복구 컨트롤러로 스크롤을 내리십시오.

Amazon Route 53 Application Recovery Controller의 다중 리전 복구 시작하기

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 사용하여 AWS 애플리케이션을 장애 조치하려면 여러 개의 애플리케이션이 있어야 합니다 AWS 리전. 시작하려면 먼저 애플리케이션이 각 지역의 사일로 복제본에 설정되어 있어야 이벤트 중에 한 지역에서 다른 지역으로 페일오버할 수 있습

니다. 그런 다음 라우팅 제어를 생성하여 애플리케이션 트래픽을 기본 애플리케이션에서 보조 애플리케이션으로 장애 조치하도록 재라우팅하여 사용자의 연속성을 유지할 수 있습니다.

> **Note**
>
> 가용 영역에 의해 격리된 애플리케이션이 있는 경우 장애 조치 복구를 위해 영역 이동 또는 영역 자동 이동을 사용하는 것이 좋습니다. 가용 영역 장애로부터 애플리케이션을 안정적으로 복구하기 위해 영역 이동 또는 영역 자동 이동을 사용하기 위한 설정은 필요하지 않습니다. 자세한 정보는 Amazon Route 53 애플리케이션 복구 컨트롤러에서 영역 이동 및 영역 자동 이동을 사용하여 애플리케이션을 복구합니다.을 참조하세요.

이벤트 중에 Route 53 ARC 라우팅 제어를 사용하여 애플리케이션을 복구하려면 서로의 복제본인 애플리케이션을 두 개 이상 설정하는 것이 좋습니다. 각 복제본 또는 셀은 을 나타냅니다. AWS 리전지역에 맞게 애플리케이션 리소스를 설정한 후에는 다음 단계를 수행하여 애플리케이션이 성공적인 복구를 위해 설정되었는지 확인하십시오.

팁: 설정을 단순화할 수 있도록 당사는 서로 독립적으로 실패하는 중복 복제본이 있는 애플리케이션을 생성하는 HashiCorp Terraform 템플릿과 Terraform 템플릿을 제공합니다 AWS CloudFormation . 템플릿에 대해 자세히 알아보고 다운로드하려면 을 참조하십시오. 예제 앱 설정

라우팅 제어 사용을 준비하려면 다음을 수행하여 애플리케이션이 복원력을 갖도록 설정되어 있는지 확인하세요.

1. 이벤트 발생 시 한 지역에서 다른 지역으로 트래픽을 페일오버할 수 있도록 각 리전에서 서로의 복제본인 애플리케이션 스택 (네트워킹 및 컴퓨팅 레이어) 의 독립된 복사본을 구축하세요. 애플리케이션 코드에 한 복제본에 장애가 발생하여 다른 복제본에 영향을 미칠 수 있는 지역 간 종속성이 없어야 합니다. 두 지역 간에 AWS 리전성공적으로 페일오버를 수행하려면 스택 경계가 지역 내에 있어야 합니다.
2. 애플리케이션에 필요한 모든 스테이트풀 데이터를 복제본 전체에 복제하십시오. AWS 데이터베이스 서비스를 사용하여 데이터를 복제할 수 있습니다.

트래픽 페일오버를 위한 라우팅 제어를 시작해 보세요.

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 사용하면 별도로 실행되는 중복 애플리케이션 사본 또는 복제본 사이에서 트래픽이 장애 조치되도록 트리거할 수 있습니다. AWS 리전장애 조치는 Amazon Route 53 데이터 플레인을 사용하여 DNS를 통해 수행됩니다.

다음 섹션에 설명된 대로 각 지역에 복제본을 설정한 후 각 복제본을 라우팅 컨트롤과 연결할 수 있습니다. 먼저, 라우팅 제어를 각 지역 복제본의 최상위 도메인 이름과 연결합니다. 그런 다음 라우팅 컨트롤에 라우팅 제어 상태 점검을 추가하여 트래픽 흐름을 켜고 끌 수 있도록 합니다. 이를 통해 애플리케이션 복제본 전반의 트래픽 라우팅을 제어할 수 있습니다.

에서 라우팅 제어 상태를 AWS Management Console 업데이트하여 트래픽을 페일오버할 수 있지만, 대신 API 또는 AWS CLI를 사용하여 Route 53 ARC 작업을 사용하여 변경하는 것이 좋습니다. API 작업은 콘솔에 종속되지 않으므로 복원력이 더 높습니다.

예를 들어 us-west-1에서 us-east-1로 지역 간에 페일오버하려면 API 작업을 `update-routing-control-state` 사용하여 상태를 to 및 to로 설정할 수 있습니다. `us-west-1` `Off` `us-east-1` `On`

애플리케이션의 장애 조치를 설정하기 위해 라우팅 제어 구성 요소를 생성하기 전에 애플리케이션이 지역 복제본으로 사일로되어 있는지 확인하여 한 지역에서 다른 지역으로 페일오버할 수 있도록 해야 합니다. 자세히 알아보고 새 애플리케이션을 사일로화하거나 예제 스택을 생성하기 시작하려면 다음 섹션을 참조하십시오.

예제 앱 설정

라우팅 제어의 작동 방식을 이해하는 데 도움이 되도록 라는 예제 애플리케이션을 제공합니다`TicTacToe`. 이 예제에서는 AWS CloudFormation 템플릿을 사용하여 프로세스를 간소화하고, 다운로드 가능한 HashiCorp Terraform AWS CloudFormation 템플릿과 샘플 앱을 함께 사용하므로 Route 53 ARC 설정 및 사용을 직접 빠르게 탐색할 수 있습니다.

샘플 앱을 배포한 후 템플릿을 사용하여 Route 53 ARC 구성 요소를 생성한 다음, 라우팅 제어를 통해 앱으로의 트래픽 흐름을 관리하는 방법을 탐색할 수 있습니다. 템플릿과 프로세스를 자체 시나리오와 애플리케이션에 맞게 조정할 수 있습니다.

- AWS CloudFormation: 샘플 애플리케이션과 AWS CloudFormation 템플릿을 시작하려면 이 Amazon S3 버킷의 README 지침을 참조하십시오. 사용 AWS CloudFormation 설명서의 AWS CloudFormation 개념을 읽으면 AWS CloudFormation 템플릿 사용에 대해 자세히 알아볼 수 있습니다.
- HashiCorp Terraform: 샘플 애플리케이션 및 Terraform 템플릿으로 시작하려면 이 Amazon S3 버킷의 README 지침을 참조하십시오. 설명서를 읽으면 Terraform 템플릿 사용에 대해 자세히 알아볼 수 있습니다. HashiCorp

Route 53 ARC에서의 라우팅 제어에 대한 모범 사례

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어에 대한 복구 및 장애 조치 준비를 위한 다음 모범 사례를 권장합니다.

주제

용도에 맞게 구축되고 수명이 긴 AWS 자격 증명을 안전하게 유지하고 항상 액세스할 수 있습니다.

재해 복구 (DR) 시나리오에서는 복구 작업에 대한 액세스 AWS 및 수행에 대한 간단한 접근 방식을 사용하여 시스템 종속성을 최소한으로 유지하십시오. 특히 DR 작업을 위해 수명이 긴 IAM 보안 인증 정보를 만들고 필요할 때 액세스할 수 있도록 보안 인증 정보를 온프레미스 물리적 금고 또는 가상 보관소에 안전하게 보관합니다. IAM을 사용하면 액세스 키, 리소스 액세스 권한 등의 보안 자격 증명을 중앙에서 관리할 수 있습니다. AWS DR 이외 작업의 경우 AWS Single Sign-On과 같은 AWS 서비스를 사용하여 페더레이션 액세스를 계속 사용하는 것이 좋습니다.

복구 클러스터 데이터 영역 API를 사용하여 Route 53 ARC에서 장애 조치 작업을 수행하기 위해 Route 53 ARC IAM 정책을 사용자에게 연결할 수 있습니다. 자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러의 ID 기반 정책 예제 섹션을 참조하세요.

페일오버와 관련된 DNS 레코드의 경우 더 낮은 TTL 값을 선택하십시오.

장애 조치 메커니즘의 일부로 변경해야 할 수 있는 DNS 레코드, 특히 상태 확인된 레코드의 경우 더 낮은 TTL 값을 사용하는 것이 좋습니다. 이 시나리오에서는 TTL을 60초 또는 120초로 설정하는 것이 일반적입니다.

DNS TTL(time to live) 설정은 새 레코드를 요청하기 전에 레코드를 캐시해야 하는 시간을 DNS 해석기에 알려줍니다. TTL을 선택하면 지연 시간과 신뢰성, 변화에 대한 응답성 사이의 절충을 이룰 수 있습니다. 레코드의 TTL이 짧을수록 DNS 해석기는 TTL이 더 자주 쿼리하도록 지정하기 때문에 레코드에 대한 업데이트를 더 빨리 알게 됩니다.

자세한 내용은 Amazon Route 53 DNS 모범 사례의 DNS 레코드에 대한 TTL 값 선택을 참조세요.

클라이언트가 엔드포인트에 연결된 상태를 유지하는 시간을 제한하세요.

라우팅 제어를 사용하여 다른 것으로 전환하는 경우 Amazon Route 53 애플리케이션 복구 컨트롤러가 애플리케이션 트래픽을 이동하는 데 사용하는 메커니즘은 DNS 업데이트입니다. AWS 리전이 업데이트로 인해 모든 새 연결이 손상된 위치에서 멀어집니다.

하지만 기존에 열려 있는 연결이 있는 클라이언트는 클라이언트가 다시 연결될 때까지 손상된 위치에 대해 요청을 계속할 수 있습니다. 빠른 복구를 위해 클라이언트가 엔드포인트에 연결된 상태를 유지하는 시간을 제한하는 것이 좋습니다.

Application Load Balancer를 사용하는 경우 `keepalive` 옵션을 사용하여 연결 지속 시간을 구성할 수 있습니다. 자세한 내용은 Application Load Balancer 사용 설명서의 HTTP 클라이언트 유지 기간을 참조하십시오.

기본적으로 애플리케이션 로드 밸런서는 HTTP 클라이언트 keepalive 기간 값을 3600초 또는 1시간으로 설정합니다. 애플리케이션의 복구 시간 목표 (예: 300초) 에 맞도록 값을 낮추는 것이 좋습니다. HTTP 클라이언트 keepalive 지속 시간을 선택할 때는 일반적으로 재연결을 더 자주 하는 것이 지연 시간에 영향을 줄 수 있는 것과 손상된 AZ 또는 지역에서 모든 클라이언트를 더 빨리 멀리 이동시키는 것 사이의 절충점이라는 점을 고려하세요.

5개의 지역 클러스터 엔드포인트와 라우팅 제어 ARN을 북마크하거나 하드 코딩하세요.

Route 53 ARC리전 클러스터 엔드포인트의 로컬 사본을 북마크에 보관하거나 엔드포인트를 재시도하는 데 사용하는 자동화 코드로 저장하는 것이 좋습니다. 장애 이벤트 중에는 매우 안정적인 데이터 영역 클러스터에서 호스팅되지 않는 Route 53 ARC API 작업을 비롯한 일부 API 작업에 액세스하지 못할 수 있습니다. DescribeClusterAPI 작업을 사용하여 Route 53 ARC 클러스터의 엔드포인트를 나열할 수 있습니다.

엔드포인트 중 하나를 임의로 선택하여 라우팅 제어 상태를 업데이트하십시오.

장애 조치가 필요한 경우 5개의 리전 클러스터 엔드포인트에서 임의의 엔드포인트를 사용하여 라우팅 제어 상태를 업데이트(및 검색)하는 것이 좋습니다. 해당 엔드포인트에 장애가 발생하면 다른 리전 엔드포인트를 각각 다시 시도합니다. 클러스터 엔드포인트 시도 예제를 포함하여 AWS SDK를 사용한 코드 예제 사용에 대한 자세한 내용은 을 참조하십시오. AWS SDK를 사용하는 애플리케이션 복구 컨트롤러의 코드 예제

콘솔이 아닌 매우 안정적인 데이터 플레인 API를 사용하여 라우팅 제어 상태를 나열하고 업데이트하십시오.

Route 53 ARC 데이터 플레인 API를 사용하여 Controls 작업을 통해 라우팅 제어 및 상태를 확인하고, 라우팅 제어 상태를 업데이트하여 작업에 따른 장애 조치를 위해 트래픽을 리디렉션할 수 있습

니다. ListRouting UpdateRoutingControlState SDK 중 하나를 사용하여 작성한 AWS CLI (이 예제에서처럼) 또는 코드를 사용할 수 있습니다. AWS Route 53 ARC는 데이터 영역에서 트래픽을 장애 조치할 때 API를 사용하여 최상의 신뢰성을 제공합니다. AWS Management Console에서 라우팅 제어 상태를 변경하는 대신 API를 사용하는 것이 좋습니다.

Route 53 ARC의 리전 클러스터 엔드포인트 중 하나에 연결하여 데이터 영역 API를 사용합니다. 엔드포인트를 사용할 수 없는 경우 다른 클러스터 엔드포인트로 연결을 시도합니다.

안전 규칙이 라우팅 제어 상태 업데이트를 차단하는 경우 이를 우회하여 업데이트하고 트래픽을 장애 조치할 수 있습니다. 자세한 정보는 안전 규칙을 재정의하여 트래픽 다시 라우팅을 참조하세요.

Route 53 ARC를 통한 장애 조치 테스트

Route 53 ARC 라우팅 제어를 사용하여 정기적으로 장애 조치를 테스트하여 기본 애플리케이션 스택에서 보조 애플리케이션 스택으로 장애 조치합니다. 추가한 Route 53 ARC 구조가 스택의 올바른 리소스와 일치하고 모두 예상대로 작동하는지 확인하는 것이 중요합니다. 환경에 Route 53 ARC를 설정한 후 이를 테스트하고, 사용자의 다운타임을 방지하기 위해 보조 시스템을 빠르게 가동하여 실행해야 하는 장애 상황이 발생하기 전에 장애 조치 환경이 준비되도록 주기적으로 계속 테스트해야 합니다.

라우팅 제어 API 작업

이 섹션에는 Amazon Route 53 애플리케이션 복구 컨트롤러에서 라우팅 제어를 설정하고 사용하는 데 사용할 수 있는 API 작업이 나열된 표와 관련 설명서 링크가 포함되어 있습니다.

에서 일반적인 라우팅 제어 구성 API 작업을 사용하는 방법의 예는 을 AWS Command Line Interface 참조하십시오 Route 53 ARC 라우팅 제어 API 작업을 다음과 함께 사용하는 예 AWS CLI.

다음 표에는 라우팅 제어 구성에 사용할 수 있는 Route 53 ARC API 작업이 관련 설명서 링크와 함께 나열되어 있습니다.

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
클러스터 생성	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	를 참조하십시오. CreateCluster
클러스터 설명	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	참조 DescribeCluster

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
클러스터 삭제	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	참조 DeleteCluster
계정의 클러스터 나열	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	참조 ListClusters
라우팅 제어 생성	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	CreateRouting컨트롤 참조
라우팅 제어 설명	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	DescribeRouting컨트롤 참조
라우팅 제어 업데이트	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	UpdateRouting컨트롤 참조
라우팅 제어 삭제	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	DeleteRouting컨트롤 참조
라우팅 제어 나열	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	ListRouting컨트롤 참조
제어판 생성	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	CreateControl패널 참조
제어판 설명	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	DescribeControl패널 참조
제어판 업데이트	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	UpdateControl패널 참조
제어판 삭제	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	DeleteControl패널 참조
제어판 나열	Route 53 ARC에서 라우팅 제어 구성 요소 생성 섹션 참조	ListControl패널 참조
안전 규칙 생성	라우팅 제어를 위한 안전 규칙 만들기 섹션 참조	CreateSafety규칙 참조

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
안전 규칙 설명	라우팅 제어를 위한 안전 규칙 만들기 섹션 참조	DescribeSafety규칙 참조
안전 규칙 업데이트	라우팅 제어를 위한 안전 규칙 만들기 섹션 참조	UpdateSafety규칙 참조
안전 규칙 삭제	라우팅 제어를 위한 안전 규칙 만들기 섹션 참조	DeleteSafety규칙 참조
안전 규칙 나열	라우팅 제어를 위한 안전 규칙 만들기 섹션 참조	ListSafety규칙 참조
연결된 Route 53 상태 확인 나열	Route 53 ARC에서 라우팅 제어 상태 확인 생성 섹션 참조	ListAssociated루트 53 참조 HealthChecks
클러스터 공유를 위한 AWS RAM 리소스 정책을 나열하세요.	Route 53 ARC의 클러스터에 대한 크로스 계정 지원 섹션 참조	GetResource정책을 참조하십시오.

다음 표에는 라우팅 제어 데이터 플레인으로 트래픽 페일오버를 관리하는 데 사용할 수 있는 일반적인 Route 53 ARC API 작업이 관련 문서 링크와 함께 나열되어 있습니다.

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
라우팅 제어 상태 가져오기	의 라우팅 제어 상태 가져오기 및 업데이트 AWS Management Console 섹션 참조	를 참조하십시오. GetRoutingControlState
라우팅 제어 나열	N/A	ListRouting컨트롤 참조
라우팅 제어 상태 업데이트	의 라우팅 제어 상태 가져오기 및 업데이트 AWS Management Console 섹션 참조	참조 UpdateRoutingControlState

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
여러 라우팅 제어 상태 업데이트	의 라우팅 제어 상태 가져오기 및 업데이트 AWS Management Console 섹션 참조	참조 UpdateRoutingControlStates

AWS SDK와 함께 이 서비스 사용

AWS 소프트웨어 개발 키트 (SDK) 는 널리 사용되는 여러 프로그래밍 언어에 사용할 수 있습니다. 각 SDK는 개발자가 선호하는 언어로 애플리케이션을 쉽게 구축할 수 있도록 하는 API, 코드 예시 및 설명서를 제공합니다.

SDK 설명서	코드 예시
AWS SDK for C++	AWS SDK for C++ 코드 예제
AWS CLI	AWS CLI 코드 예제
AWS SDK for Go	AWS SDK for Go 코드 예제
AWS SDK for Java	AWS SDK for Java 코드 예제
AWS SDK for JavaScript	AWS SDK for JavaScript 코드 예제
AWS SDK for Kotlin	AWS SDK for Kotlin 코드 예제
AWS SDK for .NET	AWS SDK for .NET 코드 예제
AWS SDK for PHP	AWS SDK for PHP 코드 예제
AWS Tools for PowerShell	PowerShell 코드 예제를 위한 도구
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 코드 예제
AWS SDK for Ruby	AWS SDK for Ruby 코드 예제
AWS SDK for Rust	AWS SDK for Rust 코드 예제
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP 코드 예제

SDK 설명서	코드 예시
AWS SDK for Swift	AWS SDK for Swift 코드 예제

이 서비스 관련 예시는 AWS SDK를 사용하는 애플리케이션 복구 컨트롤러의 코드 예제를 참조하세요.

> **예제 사용 가능 여부**
>
> 필요한 예제를 찾을 수 없습니까? 이 페이지 하단의 피드백 제공 링크를 사용하여 코드 예시를 요청하세요.

Route 53 ARC 라우팅 제어 API 작업을 다음과 함께 사용하는 예 AWS CLI

이 단원에서는 API 작업을 사용하는 Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어 기능을 사용하기 AWS Command Line Interface 위해 를 사용하여 라우팅 제어를 사용하는 간단한 애플리케이션 예제를 살펴봅니다. 이 예제는 CLI를 사용하여 라우팅 제어 작업을 수행하는 방법에 대한 기본적인 이해를 돕기 위한 것입니다.

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 사용하면 별도의 AWS 리전 가용 영역 또는 가용 영역에서 실행되는 중복 애플리케이션 사본 또는 복제본 사이에서 트래픽 장애 조치를 트리거할 수 있습니다.

라우팅 제어를 클러스터에 프로비저닝되는 컨트롤 패널이라는 그룹으로 구성합니다. Route 53 ARC 클러스터는 글로벌 배포되는 리전별 엔드포인트 세트입니다. 클러스터 엔드포인트는 라우팅 제어 상태를 설정하고 검색하는 데 사용할 수 있는 고가용성 API를 제공합니다. 라우팅 제어 기능의 구성 요소에 대한 자세한 내용은 라우팅 제어 구성 요소 섹션을 참조하세요.

> **Note**
>
> Route 53 ARC는 여러 AWS 리전엔드포인트를 지원하는 글로벌 서비스입니다. 하지만 대부분의 Route 53 ARC CLI 명령에서는 미국 서부 (오레곤) 리전을 지정해야 합니다. 즉, 파라미터를 `--region us-west-2` 지정해야 합니다. 예를 들어 복구 그룹, 제어 패널 및 클러스터를 생성할 때 `region` 파라미터를 사용하십시오.
>
> 클러스터를 생성할 때 Route 53 ARC는 리전 엔드포인트 세트를 제공합니다. 라우팅 제어 상태를 가져오거나 업데이트하려면 CLI 명령에 리전 엔드포인트 (AWS 리전 및 엔드포인트 URL) 를 지정해야 합니다.

사용에 대한 자세한 내용은 AWS CLI 명령 AWS CLI참조를 참조하십시오. 라우팅 제어 API 작업 목록은 라우팅 제어 API 작업 및 을 참조하십시오 라우팅 제어 API 작업.

먼저 클러스터를 만드는 것부터 시작하여 라우팅 제어를 사용하여 장애 조치를 관리하는 데 필요한 구성 요소를 만들어 보겠습니다.

라우팅 제어 구성 요소를 설정합니다.

첫 번째 단계는 클러스터 생성입니다. Route 53 ARC 클러스터는 다섯 개의 엔드포인트에 각각 하나씩 있는 다섯 개의 AWS 리전엔드포인트 세트입니다. Route 53 ARC 인프라는 이러한 엔드포인트가 조화롭게 작동하도록 지원하여 장애 조치 작업의 고가용성 및 순차적 일관성을 보장합니다.

1. 클러스터 생성

1a. 클러스터를 생성합니다.

```
aws route53-recovery-control-config --region us-west-2 create-cluster --cluster-name
 NewCluster
```

```
{
    "Cluster": {
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "Name": "NewCluster",
        "Status": "PENDING"
    }
}
```

Route 53 ARC 리소스를 처음 생성하면 클러스터가 생성되는 동안 PENDING 상태가 됩니다. describe-cluster를 호출하여 진행 상황을 확인할 수 있습니다.

1b. 클러스터를 설명합니다.

```
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::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "ClusterEndpoints":[
```

```
            {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
            {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
            {"Endpoint": "https://host-cccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
            {"Endpoint": "https://host-dddddd.us-west-2.example.com", "Region":"us-
west-2"},
            {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
        ]
        "Name": "NewCluster",
        "Status": "DEPLOYED"
    }
}
```

DEPLOYED 상태가 되면 Route 53 ARC는 사용자가 상호 작용할 수 있는 엔드포인트 세트를 포함하는 클러스터를 성공적으로 생성한 것입니다. `list-clusters`를 호출하여 모든 클러스터를 나열할 수 있습니다.

1c. 클러스터를 나열합니다.

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

```
{
    "Clusters": [
        {
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/1234abcd-abcd-1234-abcd-1234abcdefgh",
            "ClusterEndpoints":[
                {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
                {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
                {"Endpoint": "https://host-cccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
                {"Endpoint": "https://host-dddddd.us-west-2.example.com", "Region":"us-
west-2"},
                {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
            ],
            "Name": "AnotherCluster",
```

```
            "Status": "DEPLOYED"
        },
        {
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "ClusterEndpoints": [
                {"Endpoint": "https://host-ffffff.us-east-1.example.com", "Region":"us-
east-1"},
                {"Endpoint": "https://host-gggggg.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
                {"Endpoint": "https://host-hhhhhh.eu-west-1.example.com", "Region":"eu-
west-1"},
                {"Endpoint": "https://host-iiiiii.us-west-2.example.com", "Region":"us-
west-2"},
                {"Endpoint": "https://host-jjjjjj.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
            ],
            "Name": "NewCluster",
            "Status": "DEPLOYED"
        }
    ]
}
```

2. 제어판 생성

제어판은 Route 53 ARC 라우팅 제어를 구성하기 위한 논리적 그룹입니다. 클러스터를 생성하면 Route 53 ARC가 `DefaultControlPanel`을 호출한 사용자를 위한 제어판을 자동으로 제공합니다. 이 제어판은 즉시 사용할 수 있습니다.

제어판은 한 클러스터에만 존재할 수 있습니다. 제어판을 다른 클러스터로 이동하려면 제어판을 삭제한 다음 두 번째 클러스터에서 생성해야 합니다. `list-control-panels`를 호출하여 계정의 모든 제어판을 볼 수 있습니다. 특정 클러스터의 제어판만 보려면 `--cluster-arn` 필드를 추가합니다.

2a. 제어판을 나열합니다.

```
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"
        }
    ]
}
```

원하는 경우 `create-control-panel`을 호출하여 제어판을 직접 만들 수도 있습니다.

2b. 제어판을 생성합니다.

```
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"
    }
}
```

Route 53 ARC 리소스를 처음 생성하면 생성되는 동안 `PENDING` 상태가 됩니다. `describe-control-panel`을 호출하여 진행 상황을 확인할 수 있습니다.

2c. 제어판을 설명합니다.

```
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. 라우팅 제어 생성

클러스터를 설정하고 제어판을 살펴보았으므로 이제 라우팅 제어를 생성할 수 있습니다. 라우팅 제어를 생성할 때 라우팅 제어를 포함할 클러스터의 Amazon 리소스 이름(ARN)을 최소한 지정해야 합니다. 또한 라우팅 제어를 위한 제어판의 ARN을 지정할 수 있습니다. 또한 제어판이 있는 클러스터를 지정해야 합니다.

제어판을 지정하지 않으면 자동으로 생성되는 제어판 `DefaultControlPanel`에 라우팅 제어가 추가됩니다.

`create-routing-control`을 호출하여 라우팅 제어를 생성합니다.

3a. 라우팅 제어를 생성합니다.

```
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"
    }
```

```
}
```

라우팅 제어는 다른 Route 53 ARC 리소스와 동일한 생성 패턴을 따르므로 설명 작업을 호출하여 진행 상황을 추적할 수 있습니다.

3b. 라우팅 제어를 설명합니다.

```
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"
    }
}
```

`list-routing-controls`를 호출하여 제어판에 라우팅 제어를 나열할 수 있습니다. 제어판 ARN이 필요합니다.

3c. 라우팅 제어를 나열합니다.

```
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"
        }
    ]
}
```

라우팅 제어 상태 작업의 다음 예제에서는 이 섹션에 두 개의 라우팅 제어(Rc1 및 Rc2)가 나열되어 있다고 가정합니다. 이 예제에서 각 라우팅 제어는 애플리케이션이 배포되는 가용 영역을 나타냅니다.

4. 안전 규칙 생성

여러 개의 라우팅 제어를 동시에 사용하는 경우 라우팅 제어를 모두 끄고 모든 트래픽 흐름을 중지하는 등 의도하지 않은 결과를 방지하기 위해 라우팅 제어를 활성화하고 비활성화할 때 몇 가지 보호 장치를 마련해야 할 수도 있습니다. 이러한 보호 조치를 만들려면 라우팅 제어 안전 규칙을 생성해야 합니다.

안전 규칙에는 어설션 규칙과 게이팅 규칙이라는 두 가지 유형이 있습니다. 안전 규칙에 대한 자세한 내용은 라우팅 제어를 위한 안전 규칙 만들기 섹션을 참조하세요.

다음 호출은 두 개의 라우팅 제어 중 하나 이상이 주어진 시간에 On으로 설정되도록 하는 어설션 규칙을 만드는 예를 제공합니다. 규칙을 만들려면 `create-safety-rule`을 `assertion-rule` 파라미터와 함께 실행합니다.

어설션 규칙 API 작업에 대한 자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 안내서를 참조하십시오 AssertionRule.

4a. 어설션 규칙을 생성합니다.

```
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
        }
    }
}
```

다음 호출은 제어판의 대상 라우팅 제어 세트에 대한 전체 “온/오프” 또는 “게이팅” 스위치를 제공하는 게이팅 규칙을 만드는 예입니다. 이를 통해 대상 라우팅 제어의 업데이트를 허용하지 않도록 할 수 있습니다. 예를 들어 자동화가 무단으로 업데이트하지 못하도록 할 수 있습니다. 이 예제에서 게이팅 스위치는 `GatingControls` 파라미터에 의해 지정된 라우팅 제어이고, 제어되거나 “게이트”되는 두 개의 라우팅 제어는 `TargetControls` 파라미터에 의해 지정됩니다.

> **Note**
>
> 게이팅 규칙을 생성하기 전에 DNS 장애 조치 레코드를 포함하지 않는 게이팅 라우팅 제어 및 DNS 장애 조치 레코드로 구성하는 대상 라우팅 제어를 생성해야 합니다.

규칙을 만들려면 `create-safety-rule`을 `gating-rule` 파라미터와 함께 실행합니다.

어설션 규칙 API 작업에 대한 자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 안내서를 참조하십시오 GatingRule.

4b. 게이팅 규칙을 생성합니다.

```
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
        }
    }
}
```

다른 라우팅 제어 리소스와 마찬가지로 데이터 플레인에 전파된 후 안전 규칙을 설명, 나열 또는 삭제할 수 있습니다.

하나 이상의 안전 규칙을 설정한 후에도 계속해서 클러스터와 상호 작용하여 라우팅 제어 상태를 설정하거나 검색할 수 있습니다. 생성한 규칙을 위반하는 `set-routing-control-state` 작업이 발생하면 다음과 비슷한 예외가 발생합니다.

```
Cannot modify control state for [0123456bbbbbbb0123456bbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbb0123456333333444444
```

첫 번째 식별자는 라우팅 제어 ARN과 연결된 제어판 ARN입니다. 두 번째 식별자는 안전 규칙 ARN과 연결된 제어판 ARN입니다.

5. 상태 확인 생성

라우팅 제어를 사용하여 트래픽을 페일오버하려면 Amazon Route 53에서 상태 확인을 생성한 다음 상태 확인을 DNS 레코드와 연결합니다. 트래픽을 페일오버하기 위해 Route 53 ARC 라우팅 컨트롤은 상태 점검을 실패로 설정하여 Route 53이 트래픽을 다시 라우팅하도록 합니다. (상태 점검은 애플리케이션의 상태를 유효하게 하는 것이 아니라 단순히 트래픽을 재라우팅하는 방법으로만 사용됩니다.)

예를 들어 두 개의 셀 (지역 또는 가용 영역) 이 있다고 가정해 보겠습니다. 하나는 애플리케이션의 기본 셀로 구성하고 다른 하나는 페일오버를 위한 보조 셀로 구성합니다.

장애 조치를 위한 상태 확인을 설정하려면 예를 들어, 다음을 수행할 수 있습니다.

1. Route 53 ARC CLI를 사용하여 각 셀에 대한 라우팅 제어를 생성합니다.
2. Route 53 CLI를 사용하여 Route 53에서 각 라우팅 제어에 대한 Route 53 ARC 상태 확인을 생성합니다.
3. Route 53 CLI를 사용하여 Route 53에서 두 개의 장애 조치 DNS 레코드를 생성하고 각 레코드에 상태 확인을 연결합니다.

5a. 각 셀에 대한 라우팅 제어를 생성합니다.

```
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. 각 라우팅 제어에 대한 상태 확인을 생성합니다.

> **Note**
>
> Amazon Route 53 CLI를 사용하여 Route 53 ARC 상태 확인을 생성합니다.

```
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. 두 장애 조치 DNS 레코드를 생성하고 각 레코드에 상태 확인을 연결합니다.

Route 53 CLI를 사용하여 Route 53에서 장애 조치 DNS 레코드를 생성합니다. 레코드를 생성하려면 Amazon Route 53 AWS CLI 명령 참조에서 change-resource-record-sets 명령에 대한 지침을 따르십시오. 레코드에서 각 셀의 DNS 값을 Route 53이 상태 확인을 위해 생성한 해당 `HealthCheckID` 값과 함께 지정합니다(6b 참조).

기본 셀의 경우:

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "primary",
    "Failover": "PRIMARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell1.yourdomain.com"
```

```
        }
    ],
    "HealthCheckId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

보조 셀의 경우:

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

이제 기본 셀에서 보조 셀로 장애 조치하려면 4b단계의 CLI 예제에 따라 `RoutingControlCell1` 상태를 `OFF`로 `RoutingControlCell2` 상태를 `ON`으로 업데이트할 수 있습니다.

를 사용하여 라우팅 제어 및 상태를 나열하고 업데이트하십시오. AWS CLI

Amazon Route 53 애플리케이션 복구 컨트롤러 리소스 (예: 클러스터, 라우팅 제어, 제어판) 를 생성한 후 클러스터와 상호 작용하여 장애 조치를 위한 라우팅 제어 상태를 나열하고 업데이트할 수 있습니다.

생성한 각 클러스터에 대해 Route 53 ARC는 클러스터 엔드포인트 세트를 5개의 AWS 리전당 하나씩 제공합니다. 라우팅 제어 상태를 검색하거나 또는 로 설정하기 위해 클러스터를 호출할 때는 이러한 리전 엔드포인트 중 하나 (AWS 리전 및 엔드포인트 URL) 를 지정해야 `On` 합니다. `Off` 를 사용하여 라우팅 제어 상태를 가져오거나 업데이트하려면 리전 엔드포인트 외에도 이 `--region` 섹션의 예와 같이 리전 엔드포인트의 항목도 지정해야 합니다. AWS CLI

모든 리전 클러스터 엔드포인트를 사용할 수 있습니다. 시스템을 지역별 엔드포인트로 교체하고 사용 가능한 각 엔드포인트로 재시도할 수 있도록 준비하는 것이 좋습니다. 클러스터 엔드포인트를 순서대로 시도하는 방법을 보여주는 코드 샘플은 SDK를 사용하는 AWS 애플리케이션 복구 컨트롤러의 작업 섹션을 참조하세요.

사용에 대한 자세한 내용은 명령 AWS CLI참조를 참조하십시오. AWS CLI 라우팅 제어 API 작업 목록 및 자세한 정보 링크는 라우팅 제어 API 작업 섹션을 참조하세요.

> **Important**
>
> Amazon Route 53 콘솔에서 라우팅 제어 상태를 업데이트할 수 있지만, AWS CLI 또는 AWS SDK를 사용하여 라우팅 제어 상태를 업데이트하는 것이 좋습니다. Route 53 ARC는 Route 53 ARC 라우팅 제어 데이터 영역을 통해 트래픽을 다시 라우팅하고 셀 간에 장애 조치를 수행하는 데 있어 최고의 신뢰성을 제공합니다. Route 53 ARC를 사용하여 장애 조치를 수행하는 방법에 대한 자세한 권장 사항은 Route 53 ARC에서의 라우팅 제어에 대한 모범 사례 섹션을 참조하세요.

라우팅 제어를 생성하면 상태가 `Off`로 설정됩니다. 즉, 트래픽이 해당 라우팅 제어의 대상 셀로 라우팅되지 않습니다. `get-routing-control-state` 명령을 실행하여 라우팅 제어의 상태를 확인할 수 있습니다.

지정할 리전 및 엔드포인트를 결정하려면 `describe-clusters` 명령을 실행하여 `ClusterEndpoints`를 확인합니다. 각 `ClusterEndpoint`에는 라우팅 제어 상태를 가져오거나 업데이트하는 데 사용할 수 있는 리전 및 해당 엔드포인트가 포함되어 있습니다. DescribeCluster복구 제어 구성 API 작업입니다. Route 53 ARC리전 클러스터 엔드포인트의 로컬 사본을 북마크에 보관하거나 엔드포인트를 재시도하는 데 사용하는 자동화 코드로 하드코딩하여 보관하는 것이 좋습니다.

1. 라우팅 제어 나열

매우 안정적인 Route 53 ARC 데이터 영역 엔드포인트를 사용하여 라우팅 제어 및 라우팅 제어 상태를 볼 수 있습니다.

1. 특정 제어판의 라우팅 제어를 나열합니다. 제어판을 지정하지 않으면 `list-routing-controls`는 클러스터의 모든 라우팅 제어를 반환합니다.

```
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. 라우팅 제어 가져오기

2. 라우팅 제어 상태를 가져옵니다.

```
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. 라우팅 컨트롤 업데이트

라우팅 제어로 제어되는 대상 엔드포인트로 트래픽을 라우팅하려면 라우팅 제어 상태를 On으로 업데이트합니다. `update-routing-control-state` 명령을 실행하여 라우팅 제어 상태를 업데이트합니다. (요청이 성공하면 응답이 비어 있습니다.)

2a. 라우팅 제어 상태를 업데이트합니다.

```
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
```

```
{}
```

한 번의 API 직접 호출로 여러 라우팅 제어를 동시에 업데이트할 수 있습니다. `update-routing-control-states` (요청이 성공하면 응답이 비어 있습니다.)

2b. 여러 라우팅 제어 상태를 한 번에 업데이트(일괄 업데이트)합니다.

```
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
```

```
{}
```

Route 53 ARC에서 라우팅 컨트롤 컴포넌트 사용하기

주제

- Route 53 ARC에서 라우팅 제어 구성 요소 생성
- Route 53 ARC에서 라우팅 제어 상태 보기 및 업데이트
- 라우팅 제어를 위한 안전 규칙 만들기

- Route 53 ARC의 클러스터에 대한 크로스 계정 지원

Route 53 ARC에서 라우팅 제어 구성 요소 생성

이 섹션에서는 Amazon Route 53 Application Recovery Controller에서 라우팅 제어 작업을 위한 클러스터, 라우팅 제어, 상태 확인 및 제어판을 생성하는 방법을 설명합니다.

먼저 라우팅 제어 및 이를 그룹화하는 데 사용하는 제어판을 호스팅할 클러스터를 생성합니다. 그런 다음 라우팅 제어 및 상태 확인을 생성하여 한 셀에서 다른 셀로 트래픽을 장애 조치하도록 다시 라우팅하여 트래픽이 백업 복제본으로 이동하도록 할 수 있습니다.

생성한 클러스터마다 시간당 요금이 부과된다는 점에 유의하세요. 애플리케이션의 복구 제어 관리를 위한 라우팅 제어 및 제어판을 호스팅하는 데는 일반적으로 하나의 클러스터만 필요합니다. 또한, 를 사용하여 AWS Resource Access Manager리소스 공유를 설정할 수 있습니다. 그러면 한 클러스터가 라우팅 제어와 여러 사람이 소유한 다른 Route 53 ARC 리소스를 호스트할 수 AWS 계정있습니다. Route 53 ARC에서의 리소스 공유에 대해 알아보려면, Route 53 ARC의 클러스터에 대한 크로스 계정 지원. 요금 정보는 Amazon Route 53 Application Recovery Controller 요금을 참조하고 Amazon Route 53까지 아래로 스크롤하세요.

라우팅 제어를 사용하여 트래픽을 장애 조치하려면 애플리케이션의 리소스에 대한 Amazon Route 53 DNS 레코드와 연결하는 라우팅 제어 상태 확인을 생성합니다. 예를 들어, 두 개의 셀이 있는데, 하나는 애플리케이션의 기본 셀로 구성했고 다른 하나는 보조 셀로 구성하여 장애 조치를 수행한다고 가정해 보겠습니다.

장애 조치를 위한 상태 확인을 설정하려면 다음을 수행합니다.

1. 각 셀에 대한 라우팅 제어를 생성합니다.
2. 각 라우팅 제어에 대한 상태 확인을 생성합니다.
3. DNS 레코드 2개(예: DNS 장애 조치 레코드 2개)를 생성하고 각 레코드에 상태 확인을 연결합니다.

라우팅 제어를 생성할 수 있는 또 다른 시나리오는 게이팅 규칙인 안전 규칙을 생성하는 경우입니다. 이 경우 라우팅 제어를 게이팅 라우팅 제어로 사용하기 때문에 상태 확인과 DNS 레코드를 라우팅 제어에 연결하지 않습니다. 자세한 정보는 라우팅 제어를 위한 안전 규칙 만들기 을 참조하세요.

Route 53 ARC 콘솔에서 라우팅 제어를 위한 구성 요소를 생성하는 단계는 이 섹션에 포함되어 있습니다. Route 53 ARC에서 복구 제어 구성 API 작업을 사용하는 방법에 대해 알아보려면 라우팅 제어 API 작업 섹션을 참조하세요.

Route 53 ARC에서 클러스터 생성

Route 53 ARC에서 라우팅 제어 및 제어 패널을 호스팅하려면 클러스터를 생성해야 합니다.

클러스터는 API 직접 호출을 실행하여 하나 이상의 라우팅 제어 상태를 업데이트하거나 가져올 수 있는 중복된 리전 엔드포인트 세트입니다. 단일 클러스터는 여러 라우팅 제어를 호스팅할 수 있습니다.

> **Important**
>
> 생성한 클러스터마다 시간당 요금이 부과된다는 점에 유의하세요. 한 클러스터는 복구 제어 관리를 위한 여러 개의 라우팅 제어 및 제어판을 호스팅할 수 있으며, 일반적으로 애플리케이션용으로도 충분합니다.

클러스터 생성

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 클러스터를 선택하십시오.
3. 생성을 선택한 후 클러스터의 이름을 입력합니다.
4. 클러스터 생성을 선택합니다.

Route 53 ARC에서 라우팅 제어 생성

트래픽을 라우팅할 셀마다 라우팅 제어를 생성합니다. 예를 들어 복구를 위해 사일로화한 리소스가 있는 애플리케이션이 있는 경우 각 가용 영역에는 셀이 하나 있고 각 AWS 리전지역 내에 가용 영역별로 셀이 중첩되어 있을 수 있습니다. 이 시나리오에서는 각 셀과 중첩된 각 셀에 대해 라우팅 제어를 생성합니다.

라우팅 제어를 생성할 때는 라우팅 제어 이름이 각 제어판 내에서 고유해야 한다는 점에 유의하세요.

트래픽을 다시 라우팅하는 데 사용할 라우팅 제어를 생성한 후에는 각 라우팅 제어를 상태 확인과 연결하여 각 셀에 연결한 DNS 레코드를 기반으로 트래픽을 셀로 라우팅할 수 있습니다. 게이팅 규칙을 안전 규칙으로 설정하고 게이팅 라우팅 제어를 생성하는 경우에는 라우팅 제어에 상태 확인을 추가하지 않습니다.

라우팅 제어 생성

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 라우팅 제어를 선택합니다.
3. 라우팅 제어 페이지에서 생성을 선택한 다음 라우팅 제어를 선택합니다.
4. 라우팅 제어의 이름을 입력하고 제어를 추가할 클러스터를 선택한 다음 기존 제어판에 추가하도록 선택합니다(기본 제어판 사용 포함). 또는 새 제어판을 생성합니다.
5. 새 제어판을 생성하려면 제어판을 생성할 클러스터를 선택한 다음 패널 이름을 입력합니다.
6. 라우팅 제어 생성을 선택합니다.
7. 단계에 따라 라우팅 제어의 이름을 지정하고 생성합니다.

Route 53 ARC에서 라우팅 제어 상태 확인 생성

트래픽을 다시 라우팅하는 데 사용할 각 라우팅 제어에 라우팅 제어 상태 확인을 연결합니다. 그런 다음 Amazon Route 53 DNS 레코드(예: 장애 조치 DNS 레코드)로 각 상태 확인을 구성합니다. 그러면 연결된 라우팅 제어의 상태를 업데이트하여 `On` 또는 `Off`로 설정함으로써 Amazon Route 53 Application Recovery Controller에서 트래픽을 간단히 다시 라우팅할 수 있습니다.

> **Note**
>
> 기존 라우팅 제어 상태 확인을 편집하여 다른 라우팅 제어에 연결할 수는 없습니다.

라우팅 제어 상태 확인 생성

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 라우팅 제어를 선택합니다.
3. 라우팅 제어 페이지에서 라우팅 제어를 선택합니다.
4. 라우팅 제어 세부 정보 페이지에서 상태 확인 생성을 선택합니다.
5. 상태 확인의 이름을 입력한 다음 생성을 선택합니다.

다음으로 Route 53 DNS 레코드를 생성하고 라우팅 제어 상태 확인을 각 레코드에 연결합니다. 예를 들어, 라우팅 제어 상태 확인을 연결하려는 DNS 장애 조치 레코드 2개가 있다고 가정해 보겠습니다.

Route 53 ARC가 라우팅 제어를 사용하여 트래픽을 올바르게 장애 조치하도록 하려면 먼저 Route 53에 2개의 장애 조치 레코드(기본 및 보조)를 생성합니다. DNS 장애 조치 레코드 구성에 대한 자세한 내용은 상태 확인 개념을 참조하세요.

기본 장애 조치 레코드를 생성할 때 값이 다음과 같아야 합니다.

```
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
```

보조 장애 조치 레코드 값은 다음과 같아야 합니다.

```
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
```

이제 장애가 있어 트래픽을 다시 라우팅하고 싶다고 가정해 보겠습니다. 이를 수행하려면 연결된 라우팅 제어 상태를 업데이트하여 기본 라우팅 제어 상태를 OFF로 변경하고 보조 라우팅 제어 상태를 ON으로 변경합니다. 그러면 관련 상태 확인에서 트래픽이 기본 복제본으로 이동하는 것을 중지하고 대신 보조 복제본으로 라우팅합니다. 라우팅 제어를 통한 트래픽 장애 조치에 대한 자세한 내용은 Route 53 ARC API를 사용하여 라우팅 제어 상태 가져오기 및 업데이트(권장) 섹션을 참조하세요.

Route 53 ARC API 작업을 사용하여 라우팅 제어 및 관련 상태 확인을 생성하는 AWS CLI 명령의 예를 보려면 을 참조하십시오 Route 53 ARC 라우팅 제어 API 작업을 다음과 함께 사용하는 예 AWS CLI.

Route 53 ARC에서 제어판 생성

Amazon Route 53 Application Recovery Controller의 제어판을 사용하여 관련된 라우팅 제어를 그룹화할 수 있습니다. 제어판에는 장애 조치 범위에 따라 애플리케이션 내의 마이크로서비스, 전체 애플리케

이션 자체 또는 애플리케이션 그룹을 나타내는 라우팅 제어가 있을 수 있습니다. 라우팅 제어를 제어판으로 그룹화하면 제어판과 함께 안전 규칙을 사용하여 트래픽 라우팅 변경을 보호할 수 있다는 이점이 있습니다.

클러스터를 생성하면 Route 53 ARC가 기본 제어판을 생성합니다. 라우팅 제어에 기본 제어판을 사용하거나 하나 이상의 제어판을 생성하여 라우팅 제어를 그룹화할 수 있습니다. 제어판 이름에는 ASCII 문자만 지원된다는 점에 유의하세요.

Route 53 ARC 콘솔에서 제어판을 생성하는 단계는 이 섹션에 포함되어 있습니다. Route 53 ARC에서 복구 제어 구성 API 작업을 사용하는 방법에 대한 자세한 내용은 라우팅 제어 API 작업 섹션을 참조하세요.

제어판 생성

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 라우팅 제어를 선택합니다.
3. 라우팅 제어 페이지에서 생성을 선택한 다음 제어판을 선택합니다.
4. 제어판을 생성할 클러스터를 선택한 후 패널 이름을 입력합니다.
5. 제어판 생성을 선택합니다.

Route 53 ARC에서 라우팅 제어 상태 보기 및 업데이트

이 섹션에서는 Amazon Route 53 Application Recovery Controller에서 라우팅 제어 상태를 확인하고 업데이트하는 방법을 설명합니다. 라우팅 제어는 복구 그룹의 셀로 향하는 트래픽 흐름을 관리하는 간단한 온-오프 스위치입니다. 셀은 일반적으로 AWS 리전리소스가 포함된 가용 영역이거나 경우에 따라 가용 영역입니다. 라우팅 제어 상태가 0n인 경우 트래픽은 해당 라우팅 제어에 의해 제어되는 셀로 흐릅니다.

라우팅 제어를 제어판로 그룹화하며, 이는 논리적인 장애 조치 그룹입니다. 예를 들어 콘솔에서 제어판을 열면 그룹화에 대한 모든 라우팅 제어를 한 번에 확인하여 트래픽이 흐르는 위치를 확인할 수 있습니다.

Route 53 ARC 콘솔에서 또는 Route 53 ARC API를 사용하여 라우팅 제어 상태를 업데이트할 수 있습니다. API를 사용하여 라우팅 제어 상태를 업데이트하는 것이 좋습니다. 먼저, Route 53 ARC는 데이터 영역의 API를 사용하여 이러한 작업을 수행할 수 있도록 매우 높은 신뢰성을 제공합니다. 애플리케이션 트래픽을 다시 라우팅함으로써 라우팅 상태 변경이 셀 전체에서 장애 조치되기 때문에 이러한 상태

를 변경할 때는 이 점이 중요합니다. 또한 API를 사용하면 연결하려는 클러스터 엔드포인트를 사용할 수 없는 경우 필요에 따라 다른 클러스터 엔드포인트에 교대로 연결을 시도할 수 있습니다.

하나의 라우팅 제어 상태를 업데이트하거나 여러 라우팅 제어 상태를 한 번에 업데이트할 수 있습니다. 예를 들어 애플리케이션의 지연 시간이 증가하는 가용 영역과 같이 하나의 셀로 트래픽이 흐르는 것을 중지하도록 하나의 라우팅 제어 상태를 `Off`로 설정할 수 있습니다. 동시에 다른 셀이나 가용 영역으로 트래픽이 흐르기 시작하도록 다른 라우팅 제어 상태를 `On`으로 설정하는 것이 좋습니다. 이 시나리오에서는 두 라우팅 제어 상태를 동시에 업데이트하여 트래픽이 계속 흐르도록 할 수 있습니다.

주제

- Route 53 ARC API를 사용하여 라우팅 제어 상태 가져오기 및 업데이트(권장)
- 의 라우팅 제어 상태 가져오기 및 업데이트 AWS Management Console

Route 53 ARC API를 사용하여 라우팅 제어 상태 가져오기 및 업데이트(권장)

AWS CLI 명령을 사용하거나 AWS SDK 중 하나와 함께 Route 53 ARC API 작업을 사용하도록 개발한 코드를 사용하여 Amazon Route 53 애플리케이션 복구 컨트롤러 API 작업을 사용하여 라우팅 제어 상태를 가져오거나 업데이트하는 것이 좋습니다. 라우팅 제어 상태 작업에는 AWS Management Console을 사용하기보다는 CLI 또는 코드 내 API 작업을 사용하는 것이 좋습니다.

Route 53 ARC는 라우팅 제어가 고가용성 클러스터에 저장되므로 API를 사용하여 라우팅 제어 상태를 업데이트하여 셀(AWS 리전) 간 장애 조치의 안정성을 극대화합니다. Route 53 ARC는 5개 리전 클러스터 엔드포인트 중 3개 이상이 항상 액세스하여 라우팅 제어 상태 변경을 수행할 수 있도록 합니다. API를 사용하여 라우팅 제어 상태를 가져오거나 변경하려면 리전 클러스터 엔드포인트 중 하나에 연결합니다. 엔드포인트를 사용할 수 없는 경우 다른 클러스터 엔드포인트 중 하나로 연결을 시도할 수 있습니다.

Route 53 콘솔에서 또는 API 작업을 사용하여 클러스터의 지역 클러스터 엔드포인트 목록을 볼 수 있습니다. DescribeCluster 정기적인 유지 관리 및 업데이트를 위해 클러스터 엔드포인트가 사용 가능 상태와 사용 불가능 상태로 순환되므로 필요에 따라 라우팅 제어 상태를 가져오고 변경하는 프로세스에서는 각 엔드포인트를 번갈아 시도해야 합니다.

Route 53 ARC API 작업을 사용하여 라우팅 제어 상태를 가져오고 업데이트하며 리전 클러스터 엔드포인트를 사용하는 데 필요한 자세한 정보와 코드 예시를 제공합니다. 자세한 내용은 다음 자료를 참조하세요.

- 리전 클러스터 엔드포인트를 순환하여 라우팅 제어 상태를 가져오고 설정하는 방법을 설명하는 코드 예제는 SDK를 사용하는 AWS 애플리케이션 복구 컨트롤러의 작업 섹션을 참조하세요.

- 를 사용하여 라우팅 제어 상태를 가져오고 AWS CLI 업데이트하는 방법에 대한 자세한 내용은 을 참조하십시오 [를 사용하여 라우팅 제어 및 상태를 나열하고 업데이트하십시오. AWS CLI](#).

의 라우팅 제어 상태 가져오기 및 업데이트 AWS Management Console

AWS Management Console에서 라우팅 제어 상태를 가져오고 업데이트할 수 있습니다. 하지만 콘솔에서는 다른 리전 클러스터 엔드포인트를 선택할 수 없다는 점에 유의하세요. 즉, Amazon Route 53 Application Recovery Controller API를 사용할 때처럼 콘솔에서 클러스터 엔드포인트를 선택하고 순환하는 프로세스는 없습니다. 또한 콘솔은 가용성이 높지 않지만 Route 53 ARC 데이터 영역은 매우 안정적입니다. 이러한 이유로 Route 53 ARC API를 사용하여 프로덕션 작업을 위한 라우팅 제어 상태를 가져오고 업데이트하는 것이 좋습니다.

Route 53 ARC를 사용하여 장애 조치를 수행하는 방법에 대한 자세한 권장 사항은 [Route 53 ARC에서의 라우팅 제어에 대한 모범 사례](#) 섹션을 참조하세요.

콘솔에서 라우팅 제어를 보고 업데이트하려면 다음 절차의 단계를 따릅니다.

라우팅 제어 상태 가져오기

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 라우팅 제어를 선택합니다.
3. 목록에서 제어판을 선택하고 라우팅 제어를 확인합니다.

하나 이상의 라우팅 제어 상태 업데이트

1. https://console.aws.amazon.com/route53/home에서 Amazon Route 53 콘솔을 엽니다.
2. Application Recovery Controller에서 라우팅 제어를 선택합니다.
3. 작업을 선택한 다음 트래픽 라우팅 변경을 선택합니다.
4. 애플리케이션의 트래픽 흐름 또는 흐름 중단 위치에 따라 하나 이상의 라우팅 제어 상태를 `Off` 또는 `On`으로 업데이트합니다.
5. 텍스트 상자에 `confirm`를 입력합니다.
6. 트래픽 라우팅 업데이트를 선택합니다.

라우팅 제어를 위한 안전 규칙 만들기

여러 개의 라우팅 컨트롤을 동시에 사용하는 경우 의도하지 않은 결과가 발생하지 않도록 보호 장치를 마련해야 할 수도 있습니다. 예를 들어, 애플리케이션의 모든 라우팅 제어를 실수로 끄면 페일 오픈 시나리오가 발생하는 것을 방지할 수 있습니다. 또는 자동화로 인해 트래픽이 다시 라우팅되지 않도록 마스터 온/오프 스위치를 구현하여 일련의 라우팅 제어를 비활성화할 수도 있습니다. Route 53 ARC에서 라우팅 제어를 위한 이와 같은 안전 장치를 설정하려면 안전 규칙을 생성합니다.

지정한 라우팅 컨트롤, 규칙 및 기타 옵션을 조합하여 라우팅 제어에 대한 안전 규칙을 구성합니다. 각 안전 규칙은 단일 제어판과 연결되지만 제어판에는 둘 이상의 안전 규칙이 있을 수 있습니다. 안전 규칙을 만들 때는 각 제어판 내에서 안전 규칙 이름이 고유해야 한다는 점에 유의하세요.

주제

- 안전 규칙 유형
- 콘솔에서 안전 규칙 생성
- 콘솔에서 안전 규칙 편집 또는 삭제
- 안전 규칙을 재정의하여 트래픽 다시 라우팅

안전 규칙 유형

안전 규칙에는 어설션 규칙과 게이팅 규칙이라는 두 가지 유형이 있으며, 이를 사용하여 다양한 방식으로 장애 조치를 보호할 수 있습니다.

어설션 규칙

어설션 규칙을 사용하면 하나 또는 일련의 라우팅 제어 상태를 변경할 때 Route 53 ARC는 규칙을 구성할 때 설정한 기준이 충족되도록 강제하며, 그렇지 않은 경우 라우팅 제어 상태가 변경되지 않습니다.

이것이 유용한 경우의 예로는 트래픽이 한 셀로 이동하는 것을 중지하고 다른 셀로 트래픽 흐름을 시작하지 않는 시나리오와 같은 페일 오픈 시나리오를 방지하는 것입니다. 이를 방지하기 위해 어설션 규칙은 제어판에 있는 일련의 라우팅 제어 중 하나 이상의 라우팅 제어가 주어진 시간에 On인지 확인합니다. 이를 통해 트래픽이 애플리케이션의 하나 이상의 리전 또는 가용 영역으로 흐르도록 할 수 있습니다.

이 기준을 적용하기 위한 어설션 규칙을 생성하는 예제 AWS CLI 명령을 보려면 에서 안전 규칙 만들기를 참조하십시오. Route 53 ARC 라우팅 제어 API 작업을 다음과 함께 사용하는 예 AWS CLI

어설션 규칙 API 작업 속성에 대한 자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 안내서를 참조하십시오 AssertionRule.

게이팅 규칙

게이팅 규칙을 사용하면 일련의 라우팅 제어에 전체 온-오프 스위치를 적용하여 해당 라우팅 제어 상태를 변경할 수 있는지 여부가 규칙에 지정된 일련의 기준에 따라 적용되도록 할 수 있습니다. 가장 간단한 기준은 스위치로 지정한 단일 라우팅 제어가 ON 또는 OFF로 설정되어 있는지 여부입니다.

이를 구현하려면 전체 스위치로 사용할 게이팅 라우팅 제어, 대상 라우팅 제어를 생성하여 다양한 리전 또는 가용 영역으로의 트래픽 흐름을 제어합니다. 그런 다음 게이팅 규칙에 대해 구성한 대상 라우팅 제어의 수동 또는 자동 상태 업데이트를 방지하기 위해 게이팅 라우팅 제어 상태를 Off로 설정합니다. 업데이트를 허용하려면 On으로 설정합니다.

이러한 종류의 전체 전환을 구현하는 게이팅 규칙을 생성하는 예제 AWS CLI 명령을 보려면 에서 안전 규칙 생성을 참조하십시오. Route 53 ARC 라우팅 제어 API 작업을 다음과 함께 사용하는 예 AWS CLI

게이팅 규칙 API 작업 속성에 대한 자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 안내서를 참조하십시오 GatingRule.

콘솔에서 안전 규칙 생성

이 섹션의 단계에서는 Route 53 ARC 콘솔에서 안전 규칙을 생성하는 방법을 설명합니다. 어설션 규칙을 생성하든 게이팅 규칙을 생성하든 단계는 비슷합니다. 차이점은 절차에 나와 있습니다.

Amazon Route 53 Application Recovery Controller에서 복구 및 라우팅 제어 API 작업을 사용하는 방법에 대한 자세한 내용은 라우팅 제어 API 작업 섹션을 참조하세요.

안전 규칙 생성

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 라우팅 제어를 선택합니다.
3. 라우팅 제어 페이지에서 제어판을 선택합니다.
4. 제어판 세부 정보 페이지에서 작업을 선택한 다음 안전 규칙 추가를 선택합니다.
5. 추가할 규칙 유형(어설션 규칙 또는 게이팅 규칙)을 선택합니다.
6. 이름을 선택하고 선택적으로 대기 기간을 변경할 수 있습니다.

7. 안전 규칙의 구성 옵션을 지정합니다.

   - 어설션 규칙의 경우 어설션된 라우팅 제어를 지정합니다.
   - 게이팅 규칙의 경우 게이팅 라우팅 제어 및 대상 라우팅 제어를 지정합니다.

   두 규칙 모두에 대해 유형 및 임계값, 규칙 반전 여부를 선택하여 규칙 구성을 지정합니다.

   > **Note**
   >
   > 어설션 규칙 지정에 대한 자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 가이드에서 AssertionRule작업을 위해 제공된 정보를 참조하십시오. 게이팅 규칙 지정에 대한 자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 가이드에서 GatingRule작업에 대해 제공된 정보를 참조하십시오.

8. 생성을 선택합니다.

콘솔에서 안전 규칙 편집 또는 삭제

이 섹션의 단계에서는 Route 53 ARC 콘솔에서 안전 규칙을 편집 또는 삭제하는 방법을 설명합니다. 이름을 변경하거나 대기 기간을 업데이트하기 위해 안전 규칙을 제한적으로만 편집할 수 있습니다. 다른 내용을 변경하려면 안전 규칙을 삭제하고 다시 생성하십시오.

Amazon Route 53 Application Recovery Controller에서 API 작업을 사용하는 방법을 알아보려면 라우팅 제어 API 작업 섹션을 참조하세요.

안전 규칙 삭제

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 라우팅 제어를 선택합니다.
3. 라우팅 제어 페이지에서 제어판을 선택합니다.
4. 제어판 세부 정보 페이지에서 안전 규칙을 선택한 다음 삭제 또는 편집을 선택합니다.

안전 규칙을 재정의하여 트래픽 다시 라우팅

구성한 안전 규칙과 함께 적용되는 라우팅 제어 안전 장치를 우회하려는 시나리오가 있습니다. 예를 들어 재해 복구를 위해 신속하게 장애 조치하고 싶을 때 하나 이상의 안전 규칙으로 인해 예기치 않게 라

우팅 제어 상태를 업데이트하여 트래픽을 다시 라우팅하지 못할 수 있습니다. 이와 같은 “break glass” 시나리오에서는 하나 이상의 안전 규칙을 재정의하여 라우팅 제어 상태를 변경하고 애플리케이션을 장애 조치할 수 있습니다.

`safety-rules-to-override`매개 변수와 함께 또는 `update-routing-control-states` AWS CLI 명령을 사용하여 라우팅 제어 상태 (또는 여러 개의 라우팅 제어 상태) 를 업데이트할 때 안전 규칙을 우회할 수 있습니다. `update-routing-control-state` 재정의하려는 안전 규칙의 Amazon 리소스 이름(ARN)으로 파라미터를 지정하거나, 쉼표로 구분된 ARN 목록을 지정하여 둘 이상의 안전 규칙을 재정의합니다.

안전 규칙이 라우팅 제어 상태 업데이트를 차단하는 경우 오류 메시지에는 업데이트를 차단한 규칙의 ARN이 포함됩니다. 따라서 ARN을 기록해 둔 다음 안전 규칙 재정의 파라미터를 사용하여 라우팅 제어 상태 CLI 명령에서 ARN을 지정할 수 있습니다.

> **Note**
>
> 업데이트 중인 라우팅 제어에 대해 둘 이상의 안전 규칙이 있을 수 있으므로 CLI 명령을 실행하여 하나의 안전 규칙 재정의로 라우팅 제어 상태를 업데이트하지만 다른 안전 규칙이 업데이트를 차단하고 있다는 오류가 발생할 수 있습니다. 업데이트 명령이 성공적으로 완료될 때까지 업데이트 명령에서 재정의할 규칙 목록에 안전 규칙 ARN을 쉼표로 구분하여 계속 추가합니다.

API 및 SDK와 함께 `SafetyRulesToOverride` 속성을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오. UpdateRoutingControlState

다음은 안전 규칙을 재정의하여 라우팅 제어 상태를 업데이트하는 CLI 명령의 두 가지 예입니다.

한 가지 안전 규칙 재정의

```
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
```

두 가지 안전 규칙 재정의

```
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
```

Route 53 ARC의 클러스터에 대한 크로스 계정 지원

Amazon Route 53 애플리케이션 복구 컨트롤러는 와 통합되어 리소스 AWS Resource Access Manager 공유를 가능하게 합니다. AWS RAM 리소스를 다른 사람과 AWS 계정 공유하거나 이를 통해 AWS Organizations공유할 수 있게 해주는 서비스입니다. Route 53 ARC의 경우 클러스터 리소스를 공유할 수 있습니다.

를 사용하면 리소스 공유를 생성하여 소유한 리소스를 공유할 수 있습니다. AWS RAM리소스 공유는 공유할 리소스 및 공유할 참여자를 지정합니다. 참여자에는 다음이 포함될 수 있습니다.

- 소유자 조직 AWS 계정 내부 또는 외부의 특정 AWS Organizations
- 조직 내 조직 단위: AWS Organizations
- 조직 전체가 AWS Organizations

에 대한 AWS RAM자세한 내용은 AWS RAM 사용 설명서를 참조하십시오.

를 AWS Resource Access Manager 사용하여 Route 53 ARC의 계정 간에 클러스터 리소스를 공유하면 하나의 클러스터를 사용하여 여러 다른 사용자가 소유한 제어판 및 라우팅 제어를 호스팅할 수 AWS 계정있습니다. 클러스터를 공유하도록 선택하면 지정한 다른 AWS 계정 사용자가 클러스터를 사용하여 자체 제어 패널 및 라우팅 제어를 호스팅할 수 있으므로 여러 팀 간에 라우팅 기능을 더 잘 제어하고 유연하게 사용할 수 있습니다.

AWS RAM AWS 고객이 리소스를 안전하게 공유할 수 있도록 지원하는 AWS 계정서비스입니다. 를 사용하면 IAM 역할 및 사용자를 사용하여 조직 또는 조직 단위 (OU) 내에서 리소스를 공유할 수 있습니다. AWS RAM AWS Organizations AWS RAM 클러스터를 공유하는 중앙 집중화되고 통제된 방법입니다.

클러스터를 공유하면 조직에 필요한 전체 클러스터 수를 줄일 수 있습니다. 공유 클러스터를 사용하면 클러스터를 실행하는 데 드는 총 비용을 여러 팀에 할당하여 더 낮은 비용으로 Route 53 ARC의 이점을 극대화할 수 있습니다. (클러스터에 호스팅되는 리소스를 생성하는 데는 소유자 또는 참여자 모두 추가 비용이 들지 않습니다.) 계정 간에 클러스터를 공유하면 여러 애플리케이션을 Route 53 ARC에 쉽게 온보딩할 수 있으며, 특히 여러 계정 및 운영 팀에 분산된 애플리케이션 수가 많은 경우 더욱 그렇습니다.

Route 53 ARC에서 크로스 계정 공유를 시작하려면 AWS RAM에서 리소스 공유를 생성합니다. 리소스 공유는 계정이 소유한 클러스터를 공유할 권한이 있는 참여자를 지정합니다. 그런 다음 참가자는 또는 AWS SDK를 사용하여 Route 53 ARC API 작업을 AWS Management Console 실행하거나 클러스터에서 제어 패널 및 라우팅 제어와 같은 리소스를 생성할 수 있습니다. AWS Command Line Interface

이 항목에서는 소유한 리소스를 공유하는 방법과 공유 리소스를 사용하는 방법을 설명합니다.

내용

클러스터 공유를 위한 사전 조건

- 클러스터를 공유하려면 클러스터를 소유해야 합니다. AWS 계정즉, 계정에서 리소스를 할당하거나 프로비저닝해야 합니다. 나와 공유된 클러스터는 공유할 수 없습니다.
- AWS Organizations의 조직 또는 조직 단위와 클러스터를 공유하려면 AWS Organizations와의 공유를 활성화해야 합니다. 자세한 내용은 AWS RAM 사용 설명서에서 AWS Organizations를 사용하여 공유 사용을 참조하세요.

클러스터 공유

소유한 클러스터를 공유하면 클러스터를 공유하도록 지정한 참여자가 클러스터에 고유한 Route 53 ARC 리소스를 생성하고 호스팅할 수 있습니다.

클러스터를 공유하려면 리소스 공유에 추가해야 합니다. 리소스 공유는 AWS 계정전반에서 리소스를 공유할 수 있게 해주는 AWS RAM 리소스입니다. 리소스 공유는 공유할 리소스 및 공유할 참여자를 지정합니다. 클러스터를 공유하기 위해 새 리소스 공유를 생성하거나 리소스를 기존 리소스 공유에 추가할 수 있습니다. 새 리소스 공유를 생성하려면 AWS RAM 콘솔을 사용하거나 AWS Command Line Interface 또는 AWS SDK와 함께 AWS RAM API 작업을 사용할 수 있습니다.

에서 조직에 속해 AWS Organizations 있고 조직 내 공유가 활성화되어 있는 경우 조직의 참여자에게 공유 클러스터에 대한 액세스 권한이 자동으로 부여됩니다. 그렇지 않으면 참여자는 리소스 공유에 참여하라는 초대장을 받고 초대를 수락한 후 공유 클러스터의 액세스 권한을 받습니다.

AWS RAM 콘솔을 사용하거나 AWS CLI 또는 SDK와 함께 AWS RAM API 작업을 사용하여 소유한 클러스터를 공유할 수 있습니다.

콘솔을 사용하여 소유한 클러스터를 공유하려면 AWS RAM

AWS RAM 사용 설명서의 리소스 공유 생성을 참조하세요.

를 사용하여 소유한 클러스터를 공유하려면 AWS CLI

create-resource-share 명령을 사용합니다.

공유 클러스터 공유 해제

클러스터 공유를 해제하면 참여자와 소유자에게 다음이 적용됩니다.

- 현재 참여자 리소스는 공유 해제된 클러스터에 계속 존재합니다.
- 참여자는 공유 해제된 클러스터의 라우팅 제어 상태를 계속 업데이트하여 애플리케이션 장애 조치를 위한 라우팅을 관리할 수 있습니다.
- 참여자는 공유 해제된 클러스터에 더 이상 새로운 리소스를 생성할 수 없습니다.
- 참여자가 공유 해제된 클러스터의 리소스를 여전히 가지고 있을 경우 소유자는 공유 클러스터를 삭제할 수 없습니다.

소유하고 있는 공유 클러스터를 공유 해제하려면 리소스 공유에서 제거합니다. AWS RAM 콘솔을 사용하거나 AWS CLI 또는 SDK와 함께 AWS RAM API 작업을 사용하여 이 작업을 수행할 수 있습니다.

콘솔을 사용하여 소유한 공유 클러스터를 공유 해제하려면 AWS RAM

AWS RAM 사용 설명서에서 리소스 공유 업데이트를 참조하세요.

를 사용하여 소유한 공유 클러스터를 공유 해제하려면 AWS CLI

disassociate-resource-share 명령을 사용합니다.

공유 클러스터 식별

소유자와 참여자는 AWS RAM에서 정보를 확인하여 공유 클러스터를 식별할 수 있습니다. Route 53 ARC 콘솔 및 AWS CLI를 사용하여 공유 리소스에 대한 정보를 얻을 수도 있습니다.

일반적으로 공유했거나 공유한 리소스에 대해 자세히 알아보려면 AWS Resource Access Manager 사용 설명서의 정보를 참조하십시오.

- 소유자는 AWS RAM을 사용하여 다른 사람과 공유하고 있는 모든 리소스를 볼 수 있습니다. 자세한 내용은 에서 공유 리소스 보기를 참조하십시오 AWS RAM.
- 참가자는 를 사용하여 공유된 모든 리소스를 볼 수 AWS RAM있습니다. 자세한 내용은 에서 공유 리소스 보기를 참조하십시오 AWS RAM.

소유자는 에서 정보를 AWS Management Console 확인하거나 AWS Command Line Interface with Route 53 ARC API 작업을 사용하여 클러스터를 공유하는지 확인할 수 있습니다.

콘솔을 사용하여 소유하고 있는 클러스터가 공유되어 있는지 확인

클러스터의 AWS Management Console세부 정보 페이지에서 클러스터 공유 상태를 참조하십시오.

소유한 클러스터를 공유하는지 확인하려면 다음을 사용하십시오. AWS CLI

get-resource-policy 명령을 사용합니다. 클러스터에 대한 리소스 정책이 있는 경우 명령은 정책에 대한 정보를 반환합니다.

참여자는 클러스터를 공유할 때 일반적으로 공유를 수락해야 합니다. 또한 클러스터의 소유자 필드에는 클러스터 소유자의 계정이 포함됩니다.

공유 클러스터에 대한 책임 및 권한

소유자에 대한 권한

소유한 클러스터를 다른 AWS 계정사람과 공유하는 경우 클러스터를 사용할 수 있는 참여자는 클러스터에 제어판, 라우팅 제어 및 기타 리소스를 만들 수 있습니다.

클러스터 소유자는 클러스터를 생성, 관리 및 삭제할 책임이 있습니다. 라우팅 제어 및 안전 규칙과 같이 참여자가 생성한 리소스를 수정하거나 삭제할 수 없습니다. 예를 들어 참여자가 만든 라우팅 제어를 업데이트하여 라우팅 제어 상태를 변경할 수 없습니다.

하지만 소유한 클러스터의 참여자가 만든 라우팅 제어의 세부 정보는 볼 수 있습니다. 예를 들어, AWS Command Line Interface 또는 AWS SDK를 사용하여 Route 53 ARC 라우팅 제어 API 작업을 호출하여 라우팅 제어 상태를 볼 수 있습니다.

참여자가 생성한 리소스를 수정해야 하는 경우 참여자는 리소스에 액세스할 수 있는 권한이 있는 역할을 IAM에서 설정하고 역할에 계정을 추가할 수 있습니다.

참여자에 대한 권한

일반적으로 참여자는 공유되는 클러스터에서 자신이 만든 제어판, 라우팅 제어, 안전 규칙 및 상태 확인을 만들고 사용할 수 있습니다. 리소스를 소유한 경우에만 공유 클러스터의 클러스터 리소스를 보거나 수정하거나 삭제할 수 있습니다. 예를 들어 참여자는 자신이 만든 제어판에 대한 안전 규칙을 만들고 삭제할 수 있습니다.

참여자에게는 다음과 같은 제한 사항이 적용됩니다.

- 참여자는 공유 클러스터를 사용하여 다른 계정에 의해 생성된 제어판을 확인, 수정, 삭제할 수 없습니다.
- 참여자는 다른 계정에 의해 공유 클러스터에서 생성된 리소스에 대한 라우팅 제어(라우팅 제어 상태 등)를 확인, 생성, 수정할 수 없습니다.
- 참여자는 공유 클러스터의 다른 계정으로 만든 안전 규칙을 생성, 수정, 확인할 수 없습니다.
- 공유 클러스터는 클러스터 소유자에게 속하므로 참여자는 공유 클러스터의 기본 제어판에 리소스를 추가할 수 없습니다.

앞서 언급한 바와 같이, 클러스터 소유자가 기본 제어판을 소유하기 때문에 참여자는 공유 클러스터의 기본 제어판에서 라우팅 제어를 생성할 수 없습니다. 하지만 클러스터 소유자는 클러스터의 기본 제어판에 액세스할 권한을 제공하는 크로스 계정 IAM 역할을 생성할 수 있습니다. 그러면 소유자는 참여자에게 역할을 수임할 권한을 부여하여 참여자가 기본 제어판에 액세스해 소유자가 역할 권한을 통해 지정한 방식대로 사용할 수 있도록 할 수 있습니다.

청구 비용

Route 53 ARC의 클러스터 소유자에게는 클러스터와 관련된 비용이 청구됩니다. 클러스터에서 호스팅되는 리소스를 생성하는 데는 클러스터 소유자 또는 참여자에게 추가 비용이 들지 않습니다.

자세한 요금 정보 및 예를 보려면 Amazon Route 53 Application Recovery Controller 요금을 참조하고 Amazon Route 53 Application Recovery Controller까지 아래로 스크롤하세요.

할당량

공유 클러스터에 액세스할 수 있는 모든 참여자가 생성한 리소스를 포함하여 공유 클러스터에 생성된 모든 리소스는 클러스터 및 기타 리소스(예: 라우팅 제어)에 적용되는 할당량에 포함됩니다. 클러스터 리소스를 공유하는 계정의 할당량이 클러스터 소유자의 할당량보다 높으면 클러스터 소유자의 할당량이 공유 계정의 할당량보다 우선합니다.

작동 방식을 더 잘 이해하려면 다음 예를 참조하십시오. 리소스 공유에서 할당량이 어떻게 작동하는지 설명하기 위해 이 예제에서 클러스터 소유자가 소유자이고 클러스터를 공유한 계정이 참여자라고 가정해 보겠습니다.

제어판 할당량

클러스터당 소유자의 전체 제어 패널에 할당량이 적용됩니다.

예를 들어, 소유자의 클러스터당 제어 패널 수 할당량이 50개이고 클러스터에 13개의 제어 패널이 있다고 가정해 보겠습니다. 이제 참가자의 할당량이 150으로 설정되어 있다고 가정해 보겠습니다. 이 시나리오에서 참가자는 공유 클러스터에 최대 37개의 컨트롤 패널 (즉, 50~13개) 만 생성할 수 있습니다.

또한 클러스터를 공유하는 다른 계정도 제어판을 만들면 이 모든 계정도 클러스터 전체 할당량인 50개 제어 패널에 포함됩니다.

라우팅 제어 할당량

라우팅 제어에는 제어판당 할당량, 클러스터당 할당량, 안전 규칙당 할당량 등 여러 할당량이 있습니다. 이러한 모든 할당량에는 소유자 할당량이 우선합니다.

예를 들어, 소유자의 클러스터당 라우팅 컨트롤 수 할당량이 300인데 클러스터에 이미 300개의 라우팅 컨트롤이 있다고 가정해 보겠습니다. 이제 참가자의 할당량을 500으로 설정했다고 가정해 보겠습니다. 이 시나리오에서 참여자는 공유 클러스터에서 새 라우팅 컨트롤을 생성할 수 없습니다.

안전 규칙, 할당량

할당량은 제어판 할당량에 따라 소유자의 안전 규칙에 적용됩니다.

예를 들어, 제어판별 안전 규칙 수에 대해 소유주의 할당량이 20이고 참여자가 이 할당량을 80으로 설정했다고 가정해 보겠습니다. 이 시나리오에서는 소유자의 하한이 우선하므로 참여자는 공유 클러스터의 제어판에 최대 20개의 안전 규칙만 생성할 수 있습니다.

라우팅 제어 할당량 목록은 을 참조하십시오. 라우팅 제어 할당량

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어에 대한 로깅 및 모니터링

Amazon Route 53 애플리케이션 복구 컨트롤러에서 라우팅 제어를 모니터링하는 데 사용하여 AWS CloudTrail 패턴을 분석하고 문제를 해결할 수 있습니다.

주제

- 를 사용하여 Route 53 ARC API 호출을 로깅합니다. AWS CloudTrail

를 사용하여 Route 53 ARC API 호출을 로깅합니다. AWS CloudTrail

Amazon Route 53 애플리케이션 복구 컨트롤러는 Route 53 ARC에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 기록을 제공하는 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail Route 53 ARC에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Route 53 ARC 콘솔로부터의 호출과 Route 53 ARC API 작업에 대한 코드 호출이 포함됩니다.

트레일을 생성하면 Route 53 ARC에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷에 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다.

에서 수집한 CloudTrail 정보를 사용하여 Route 53 ARC에 대한 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Route 53 ARC 정보는 CloudTrail

CloudTrail 계정을 생성할 AWS 계정 때 활성화됩니다. Route 53 ARC에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 CloudTrail 이벤트 기록 작업을 참조하십시오.

Route 53 ARC에 대한 이벤트를 AWS 계정포함하여 귀하의 이벤트에 대한 지속적인 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Route 53 ARC 작업은 Amazon Route 53 애플리케이션 복구 컨트롤러용 복구 준비 API 참조 가이드, Amazon Route 53 애플리케이션 복구 컨트롤러용 복구 제어 구성 API 참조 가이드, Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 가이드에 의해 CloudTrail 기록되고 문서화됩니다. 예를 들어`CreateCluster`, 에 대한 호출 `UpdateRoutingControlState` 및 `CreateRecoveryGroup` 작업은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail UserIdentity 요소를 참조하십시오.

이벤트 기록에서 Route 53 ARC 이벤트 확인하기

CloudTrail 이벤트 기록에서 최근 이벤트를 볼 수 있습니다. Route 53 ARC API 요청에 대한 이벤트를 확인하려면 콘솔 상단의 리전 선택기에서 미국 서부(오레곤)를 선택해야 합니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록 작업을 참조하십시오.

Route 53 ARC 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 라우팅 제어 구성 `CreateCluster` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "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"
}
```

다음 예제는 라우팅 제어 UpdateRoutingControlState 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "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"
}
```


라우팅 제어를 위한 Identity 및 Access Management

AWS Identity and Access Management (IAM) 은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM 관리자는 누가 Route 53 ARC 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

내용

- Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어가 IAM과 함께 작동하는 방식
- Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 ID 기반 정책 예제
- AWS Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 관리형 정책

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어가 IAM과 함께 작동하는 방식

Amazon Route 53 애플리케이션 복구 컨트롤러에서 IAM을 사용하여 라우팅 제어에 대한 액세스를 관리하기 전에, 라우팅 제어와 함께 사용할 수 있는 IAM 기능에 대해 알아보십시오.

Amazon Route 53 애플리케이션 복구 컨트롤러에서 라우팅 제어와 함께 사용할 수 있는 IAM 기능

IAM 특성	라우팅 제어 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 연결 역할	아니요

AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 개괄적으로 파악하려면 IAM 사용 설명서의 IAM과 연동되는AWS 서비스를 참조하십시오.

Route 53 ARC의 자격 증명 기반 정책

ID 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는

역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

라우팅 제어를 위한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 ID 기반 정책 예제

라우팅 제어 내의 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다.

라우팅 제어를 위한 정책 조치

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

라우팅 제어를 위한 Route 53 ARC 작업 목록을 보려면 서비스 권한 부여 참조의 Amazon Route 53 복구 제어에서 정의한 작업 및 Amazon Route 53 복구 클러스터에서 정의한 작업을 참조하십시오.

라우팅 제어를 위한 Route 53 ARC의 정책 작업은 작업 중인 API에 따라 작업 전에 다음 접두사를 사용합니다.

```
route53-recovery-control-config
route53-recovery-cluster
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다. 예를 들어 다음을 수행할 수 있습니다.

```
"Action": [
      "route53-recovery-control-config:action1",
      "route53-recovery-control-config:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Describe라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "route53-recovery-control-config:Describe*"
```

라우팅 제어를 위한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 ID 기반 정책 예제

Route 53 ARC의 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

서비스 권한 부여 참조에서 Route 53 ARC와 관련된 다음 정보를 확인할 수 있습니다.

리소스 유형 및 해당 ARN 목록과 각 리소스의 ARN으로 지정할 수 있는 작업 목록을 보려면 서비스 권한 부여 참조에서 다음 항목을 참조하세요.

- Amazon Route 53 Recovery Controls에 의해 정의된 작업
- Amazon Route 53 복구 클러스터에서 정의한 작업

라우팅 제어를 위한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 ID 기반 정책 예제

Route 53 ARC에 대한 정책 조건 키

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition`요소를 지정하거나 단일 `Condition`요소에서 여러 키를 지정하는 경우 AWS 는 논리적 `AND`태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

라우팅 제어를 위한 Route 53 ARC 조건 키 목록을 보려면 서비스 권한 부여 참조의 다음 항목을 참조하십시오.

- Amazon Route 53 Recovery Controls에 사용되는 조건 키
- Amazon Route 53 Recovery Cluster에 사용되는 조건 키

조건 키와 함께 사용할 수 있는 작업 및 리소스를 보려면 서비스 권한 부여 참조에서 다음 항목을 참조하세요.

- 리소스 유형 및 해당 ARN 목록을 보려면 Amazon Route 53 복구 제어에서 정의한 작업 및 Amazon Route 53 복구 클러스터에서 정의한 작업을 참조하십시오.

- 각 리소스의 ARN으로 지정할 수 있는 작업 목록을 보려면 Amazon Route 53 복구 제어에서 정의한 리소스 및 Amazon Route 53 복구 클러스터에서 정의한 리소스를 참조하십시오.

라우팅 제어를 위한 Route 53 ARC ID 기반 정책의 예를 보려면 다음을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 ID 기반 정책 예제

Route 53 ARC의 액세스 제어 목록(ACL)

ACL 지원	아니요

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Route 53 ARC과 함께하는 ABAC(속성 기반 액세스 제어)

ABAC(정책 내 태그) 지원	부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Route 53 ARC 라우팅 제어에는 ABAC에 대한 다음과 같은 지원이 포함됩니다.

- 복구 제어 구성은 ABAC를 지원합니다.
- 복구 클러스터는 ABAC를 지원하지 않습니다.

Route 53 ARC에서 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

Route 53 ARC의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원	예

IAM 개체 (사용자 또는 역할) 를 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 정책은 보안 주체에게 권한을 부여합니다. 일부 서비스를 사용할 때는 다른 서비스에서 다른 작업을 트리거하는 작업을 수행할 수 있습니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다.

작업에 정책에서 추가 종속 작업이 필요한지 여부를 확인하려면 서비스 권한 부여 참조를 참조하세요.

- Amazon Route 53 Recovery Cluster
- Amazon Route 53 Recovery Controls

Route 53 ARC의 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조합니다.

Route 53 ARC의 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 서비스에 연결된 서비스 역할의 한 유형입니다. AWS 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 표시되며 서비스에서 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

라우팅 제어는 서비스 연결 역할을 사용하지 않습니다.

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 ID 기반 정책 예제

기본적으로 사용자 및 역할에는 Route 53 ARC 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 비롯하여 Route 53 ARC에 의해 정의되는 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 Amazon Route 53 Application Recovery Controller에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- 예: 라우팅 제어를 위한 Route 53 ARC 콘솔 액세스
- 예: 라우팅 제어 구성을 위한 Route 53 ARC API 작업

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Route 53 ARC 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

예: 라우팅 제어를 위한 Route 53 ARC 콘솔 액세스

Amazon Route 53 Application Recovery Controller 콘솔에 액세스하려면 최소한의 권한 세트가 있어야 합니다. 이러한 권한을 통해 내 Route 53 ARC 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 AWS

계정합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

특정 API 작업에만 액세스를 허용할 때 사용자와 역할이 Route 53 ARC 콘솔을 계속 사용할 수 있도록 하려면 Route 53 ARC에 대한 `ReadOnly` AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 Route 53 ARC Route 53 ARC 관리형 정책 페이지 또는 IAM 사용 설명서의 사용자에 대한 권한 추가를 참조하세요.

사용자에게 콘솔을 통해 Route 53 ARC 라우팅 제어 기능을 사용할 수 있는 전체 액세스 권한을 부여하려면 다음과 같은 정책을 사용자에게 연결하여 Route 53 ARC 라우팅 제어 리소스 및 작업을 구성할 수 있는 모든 권한을 사용자에게 부여하십시오.

```
{
    "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": "*"
        }
    ]
}
```

예: 라우팅 제어 구성을 위한 Route 53 ARC API 작업

사용자가 Route 53 ARC API 작업을 사용하여 Route 53 ARC 라우팅 제어 구성을 사용할 수 있도록 하려면 아래 설명과 같이 사용자가 작업해야 하는 API 작업에 해당하는 정책을 연결하십시오.

복구 제어 구성을 위한 API 작업을 수행하려면 다음과 같은 정책을 사용자에게 연결하십시오.

```
{
    "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": "*"
        }
    ]
}
```

복구 클러스터 데이터 플레인 API를 사용하여 Route 53 ARC 라우팅 제어에서 작업 (예: 재해 발생 시 장애 조치가 가능하도록 라우팅 제어 상태 업데이트) 을 수행하려면 다음과 같은 Route 53 ARC IAM 정책을 IAM 사용자에게 연결할 수 있습니다.

`AllowSafetyRuleOverride` 부울은 라우팅 제어를 위한 보호 장치로 구성된 안전 규칙을 재정의할 수 있는 권한을 부여합니다. 이 권한은 “break glass” 시나리오에서 재해나 기타 긴급한 장애 조치 시나리오에서 보호 장치를 우회하기 위해 필요할 수 있습니다. 예를 들어 운영자는 재해 복구를 위해 신속하게 장애 조치를 취해야 할 수 있으며 하나 이상의 안전 규칙으로 인해 트래픽을 다시 라우팅하는 데 필요한 라우팅 제어 상태 업데이트가 예기치 않게 차단될 수 있습니다. 이 권한을 통해 운영자는 라우팅 제어 상태를 업데이트하기 위해 API를 호출할 때 재정의할 안전 규칙을 지정할 수 있습니다. 자세한 정보는 안전 규칙을 재정의하여 트래픽 다시 라우팅을 참조하세요.

운영자가 복구 클러스터 데이터 플레인 API를 사용할 수 있도록 허용하되 안전 규칙은 무시하지 않도록 하려면 boolean to를 사용하여 다음과 같은 정책을 연결할 수 있습니다. `AllowSafetyRuleOverrides` `false` 운영자가 안전 규칙을 무시할 수 있도록 하려면 boolean을 로 설정하십시오. `AllowSafetyRuleOverrides` `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 Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 관리형 정책

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonRoute 53 RecoveryControlConfigFullAccess

`AmazonRoute53RecoveryControlConfigFullAccess`를 IAM 엔터티에 연결할 수 있습니다. 이 정책은 Route 53 ARC의 복구 제어 구성 작업에 대한 전체 액세스 권한을 부여합니다. 복구 제어 구성 작업에 대한 전체 액세스가 필요한 IAM 사용자 및 다른 보안 주체에 이 정책을 연결합니다.

재량에 따라 추가 Amazon Route 53 작업에 대한 액세스 권한을 추가하여 사용자가 라우팅 제어에 대한 상태 확인을 생성할 수 있도록 할 수 있습니다. 예를 들어, `route53:GetHealthCheck`, `route53:CreateHealthCheck`, `route53:DeleteHealthCheck`, `route53:ChangeTagsForResource` 작업 중 하나 이상에 대한 권한을 허용할 수 있습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 RecoveryControlConfigFullAccess 참조의 AmazonRoute 53을 참조하십시오.

AWS 관리형 정책: AmazonRoute 53 RecoveryControlConfigReadOnlyAccess

`AmazonRoute53RecoveryControlConfigReadOnlyAccess`를 IAM 엔터티에 연결할 수 있습니다. 라우팅 제어 및 안전 규칙 구성을 확인해야 하는 사용자에게 유용합니다. 이 정책은 Route 53 ARC의 복구 제어 구성 작업에 대한 읽기 전용 액세스 권한을 부여합니다. 이러한 사용자는 복구 제어 리소스를 생성, 업데이트 또는 삭제할 수 없습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 RecoveryControlConfigReadOnlyAccess 참조의 AmazonRoute 53을 참조하십시오.

AWS 관리형 정책: AmazonRoute 53 RecoveryClusterFullAccess

`AmazonRoute53RecoveryClusterFullAccess`를 IAM 엔터티에 연결할 수 있습니다. 이 정책은 Route 53 ARC에서 클러스터 데이터 영역 작업에 대한 전체 액세스 권한을 부여합니다. 라우팅 제어 상태 업데이트 및 검색에 대한 전체 액세스가 필요한 IAM 사용자 및 다른 보안 주체에 이 정책을 연결합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 RecoveryClusterFullAccess 참조의 AmazonRoute 53을 참조하십시오.

AWS 관리형 정책: AmazonRoute 53 RecoveryClusterReadOnlyAccess

`AmazonRoute53RecoveryClusterReadOnlyAccess`를 IAM 엔터티에 연결할 수 있습니다. 이 정책은 Route 53 ARC의 클러스터 데이터 영역에 대한 읽기 전용 액세스 권한을 부여합니다. 이러한 사용자는 라우팅 제어 상태를 검색할 수 있지만 업데이트할 수는 없습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 RecoveryClusterReadOnlyAccess 참조의 AmazonRoute 53을 참조하십시오.

라우팅 제어를 위한 AWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Route 53 ARC의 라우팅 제어에 대한 AWS 관리형 정책 업데이트에 대한 자세한 내용은 을 참조하십시오Amazon Route 53 애플리케이션 복구 컨트

롤러의 AWS 관리형 정책 업데이트. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 Route 53 ARC 문서 기록 페이지에서 RSS 피드를 구독합니다.

라우팅 제어 할당량

Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어에는 다음과 같은 할당량 (이전에는 한도라고 함) 이 적용됩니다.

개체	할당량
계정당 클러스터 수	2
클러스터당 제어판 수	50
제어판의 라우팅 제어 수	100
클러스터당 총 라우팅 제어 수(모든 제어판)	300
제어판당 안전 규칙 수	20
작업 호출당 라우팅 제어 수 UpdateRoutingControlStates	10
클러스터 엔드포인트에 대한 변경 API 직접 호출 수(초당)	3

Amazon Route 53 Application Recovery Controller의 준비 확인

Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 검사를 통해 애플리케이션과 리소스가 복구 준비가 되었는지 여부를 파악할 수 있습니다. Route 53 ARC에서 AWS 애플리케이션을 모델링하고 준비 검사를 생성한 후, 검사에서 AWS 리소스 할당량, 용량, 네트워크 라우팅 정책과 같은 애플리케이션에 대한 정보를 지속적으로 모니터링합니다. 그런 다음 애플리케이션 복제본으로 페일오버하고 이벤트 복구를 수행하는 기능에 영향을 줄 수 있는 변경 사항에 대해 알림을 받도록 선택할 수 있습니다.

준비 상태 검사를 통해 다중 지역 애플리케이션을 장애 조치 트래픽을 처리하도록 확장되고 구성된 상태로 유지 관리할 수 있는지 지속적으로 확인할 수 있습니다.

이 장에서는 복구 그룹과 애플리케이션을 설명하는 셀을 생성하여 Route 53 ARC에서 애플리케이션을 모델링하여 준비 검사가 작동할 수 있는 구조를 설정하는 방법을 설명합니다. 그런 다음 단계에 따라 준비 상태 검사 및 준비 범위를 추가하여 Route 53 ARC가 애플리케이션의 준비 상태를 감사할 수 있도록 할 수 있습니다.

준비 확인을 생성한 후 리소스의 준비 확인을 모니터링할 수 있습니다. 준비 검사를 통해 프로덕션 애플리케이션의 용량, 라우팅 정책 및 기타 구성 세부 정보를 반영하여 대기 애플리케이션 복제본과 해당 리소스가 프로덕션 복제본과 지속적으로 일치하는지 확인할 수 있습니다. 복제본이 일치하지 않는 경우 용량을 추가하거나 구성을 변경하여 애플리케이션 복제본이 다시 정렬되도록 할 수 있습니다.

> **Important**
>
> 준비 확인은 애플리케이션 복제본 구성과 런타임 상태가 일치하는지 지속적으로 확인하는 데 가장 유용합니다. 준비 확인을 사용하여 프로덕션 복제본이 정상인지 여부를 나타내서는 안 되며, 준비 확인을 재해 발생 시 장애 조치의 주요 트리거로 삼아서도 안 됩니다.

Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 확인이란 무엇입니까?

Route 53 ARC에서 준비 상태를 지속적으로 (1분 간격으로) 검사하면 검사에 포함된 리소스의 AWS 프로비저닝된 용량, 서비스 할당량, 스로틀 한도, 구성 및 버전 불일치에 대한 불일치를 지속적으로 (1분 간격으로) 감사합니다. 준비 확인을 통해 이러한 차이를 알려주므로 각 복제본이 동일한 구성 설정과 동일한 런타임 상태를 갖는지 확인할 수 있습니다. 준비 확인을 통해 전체 복제본의 구성된 용량이 일정한지 확인할 수는 있지만 복제본의 용량을 사용자 대신 결정할 것이라고 기대해서는 안 됩니다. 예를 들어, 다른 셀을 사용할 수 없을 때 관리할 수 있는 충분한 버퍼 용량을 각 복제본에 할당하여 오토 스케일링의 크기를 조정할 수 있도록 애플리케이션 요구 사항을 이해해야 합니다.

할당량의 경우, Route 53 ARC가 준비 확인으로 불일치를 감지하면 높은 할당량에 맞춰 더 낮은 할당량을 늘려 복제본의 할당량을 조정하는 조치를 취할 수 있습니다. 할당량이 일치하면 준비 확인 상태가 `READY`로 표시됩니다. (이는 즉각적인 업데이트 프로세스가 아니며 총 시간은 특정 리소스 유형 및 기타 요인에 따라 달라집니다.)

첫 번째 단계는 준비 확인을 설정하여 애플리케이션을 나타내는 복구 그룹을 만드는 것입니다. 각 복구 그룹에는 개별 장애 억제 장치 또는 애플리케이션 복제본에 대한 셀이 포함됩니다. 그런 다음 애플리케

이션의 각 리소스 유형에 대한 리소스 세트를??? 만들고 준비 확인을 리소스 세트와 연결합니다. 마지막으로 리소스를 준비 범위와 연결하여 복구 그룹(애플리케이션) 또는 개별 셀(복제본, 리전 또는 가용 영역(AZ)))의 리소스에 대한 준비 확인을 수행할 수 있습니다.

준비 확인(즉, READY 또는 NOT READY)은 준비 확인 범위에 속하는 리소스 및 리소스 유형에 대한 규칙 세트를 기반으로 합니다. 각 리소스 유형에는 준비 규칙 세트가 있으며, Route 53 ARC 확인은 리소스의 준비 확인을 감사하는 데 사용합니다. 리소스가 READY인지 여부는 각 준비 규칙의 정의 방식에 따라 결정됩니다. 모든 준비 규칙은 리소스를 평가하지만 일부는 리소스를 서로 비교하고 일부는 리소스 세트의 각 리소스에 대한 특정 정보를 살펴봅니다.

준비 검사를 추가하면 Route 53 ARC API 작업을 사용하거나, 사용하거나 AWS Management Console, Route 53 ARC API 작업을 사용하는 EventBridge 등 여러 방법 중 하나로 준비 상태를 모니터링할 수 있습니다. 또한 셀 준비 및 애플리케이션 준비를 포함하여 다양한 컨텍스트에서 리소스의 준비 상태를 모니터링할 수 있습니다. Route 53 ARC의 교차 계정 권한 부여 기능을 사용하면 단일 AWS 계정에서 분산 리소스를 더 쉽게 설정하고 모니터링할 수 있습니다.

준비 검사를 통한 애플리케이션 복제본 모니터링

Route 53 ARC는 준비 확인을 통해 각 복제본이 동일한 구성 설정과 동일한 런타임 상태인지 확인하여 애플리케이션 복제본을 감사합니다. 준비 상태 검사는 애플리케이션의 AWS 리소스 용량, 구성, AWS 할당량 및 라우팅 정책을 지속적으로 감사하며, 이 정보를 사용하여 복제본이 페일오버에 대비할 준비가 되었는지 확인할 수 있습니다. 준비 상태 검사를 통해 복구 환경을 확장하고 필요할 때 페일오버할 수 있도록 구성할 수 있습니다.

다음 섹션에서는 준비 확인의 작동 방식에 대한 자세한 내용을 제공합니다.

준비 검사 및 애플리케이션 복제본

복구에 대비하려면 다른 가용 영역 또는 지역의 장애 조치 트래픽을 흡수할 수 있도록 복제본에 충분한 예비 용량을 항상 유지해야 합니다. Route 53 ARC는 지속적으로(1분에 한 번) 애플리케이션을 검사하여 프로비저닝된 용량이 모든 가용 영역 또는 리전에서 일치하는지 확인합니다.

Route 53 ARC가 검사하는 용량에는 Amazon EC2 인스턴스 수, Aurora 읽기 및 쓰기 용량 단위, Amazon EBS 볼륨 크기 등이 포함됩니다. 리소스 값에 맞게 기본 복제본의 용량을 확장했지만 대기 복제본의 해당 값도 늘리는 것을 잊은 경우, Route 53 ARC가 불일치를 감지하여 기본 복제본의 값을 늘릴 수 있습니다.

> **Important**
>
> 준비 확인은 애플리케이션 복제본 구성과 런타임 상태가 일치하는지 지속적으로 확인하는 데 가장 유용합니다. 준비 확인을 사용하여 프로덕션 복제본이 정상인지 여부를 나타내서는 안 되며, 준비 확인을 재해 발생 시 장애 조치의 주요 트리거로 삼아서도 안 됩니다.

활성-대기 구성에서 모니터링 및 상태 확인 시스템을 기반으로 셀에서 장애 조치를 취할지 아니면 셀로 장애 조치할지 결정해야 하며, 이러한 시스템에 대한 보완 서비스로서 준비 확인을 고려해야 합니다. Route 53 ARC 준비 확인은 가용성이 높지 않으므로 가동 중단 중에 액세스할 수 있는 확인에 의존해서는 안 됩니다. 또한 재해가 발생하는 동안에는 확인된 리소스를 사용하지 못할 수도 있습니다.

특정 셀 (AWS 지역 또는 가용 영역) 또는 전체 애플리케이션의 애플리케이션 리소스에 대한 준비 상태를 모니터링할 수 있습니다. 에서 규칙을 생성하여 준비 상태 확인 상태가 (예: 로`Not ready`) 변경될 때 알림을 받을 수 있습니다. EventBridge 자세한 정보는 Amazon에서 Route 53 ARC에서 준비 상태 확인 사용하기 EventBridge을 참조하세요. 또는 와 같은 API 작업을 사용하여 준비 상태를 볼 수도 있습니다. AWS Management Console`get-recovery-readiness` 자세한 정보는 준비 검사 API 작업을 참조하세요.

준비 확인 작동 방식

Route 53 ARC는 준비 확인을 통해 각 복제본이 동일한 구성 설정과 동일한 런타임 상태인지 확인하여 애플리케이션 복제본을 감사합니다.

예를 들어 복구에 대비하려면 다른 가용 영역 또는 리전의 장애 조치 트래픽을 흡수할 수 있을 만큼 충분한 여유 용량을 항상 유지해야 합니다. Route 53 ARC는 지속적으로(1분에 한 번) 애플리케이션을 검사하여 프로비저닝된 용량이 모든 가용 영역 또는 리전에서 일치하는지 확인합니다. Route 53 ARC가 검사하는 용량에는 Amazon EC2 인스턴스 수, Aurora 읽기 및 쓰기 용량 단위, Amazon EBS 볼륨 크기 등이 포함됩니다. 리소스 값에 맞게 기본 복제본의 용량을 확장했지만 대기 복제본의 해당 값도 늘리는 것을 잊은 경우, Route 53 ARC가 불일치를 감지하여 기본 복제본의 값을 늘릴 수 있습니다.

> **Important**
>
> 준비 확인은 애플리케이션 복제본 구성과 런타임 상태가 일치하는지 지속적으로 확인하는 데 가장 유용합니다. 준비 확인을 사용하여 프로덕션 복제본이 정상인지 여부를 나타내서는 안 되며, 준비 확인을 재해 발생 시 장애 조치의 주요 트리거로 삼아서도 안 됩니다.

활성-대기 구성에서 모니터링 및 상태 확인 시스템을 기반으로 셀에서 장애 조치를 취할지 아니면 셀로 장애 조치할지 결정해야 하며, 이러한 시스템에 대한 보완 서비스로서 준비 확인을 고려해야 합니다. Route 53 ARC 준비 확인은 가용성이 높지 않으므로 가동 중단 중에 액세스할 수 있는 확인에 의존해서는 안 됩니다. 또한 재해가 발생하는 동안에는 확인된 리소스를 사용하지 못할 수도 있습니다.

특정 셀 (AWS 지역 또는 가용 영역) 또는 전체 애플리케이션의 애플리케이션 리소스에 대한 준비 상태를 모니터링할 수 있습니다. 에서 규칙을 생성하여 준비 상태 확인 상태가 (예: 로`Not ready`) 변경될 때 알림을 받을 수 있습니다. EventBridge 자세한 정보는 Amazon에서 Route 53 ARC에서 준비 상태 확인 사용하기 EventBridge을 참조하세요. 또는 와 같은 API 작업을 사용하여 준비 상태를 볼 수도 있습니다. AWS Management Console`get-recovery-readiness` 자세한 정보는 준비 검사 API 작업을 참조하세요.

준비 규칙이 준비 상태를 결정하는 방법

Route 53 ARC 준비 검사는 각 리소스 유형에 대해 사전 정의된 규칙과 해당 규칙이 정의된 방식을 기반으로 준비 상태를 결정합니다. Route 53 ARC에는 지원하는 각 리소스 유형에 대한 규칙 그룹이 하나씩 포함되어 있습니다. 예를 들어 Route 53 ARC에는 Amazon Aurora 클러스터, 오토 스케일링 등에 대한 준비 규칙 그룹이 있습니다. 일부 준비 규칙은 세트의 리소스를 서로 비교하고 일부는 리소스 세트의 각 리소스에 대한 특정 정보를 살펴봅니다.

준비 규칙 또는 규칙 그룹은 추가, 편집, 제거할 수 없습니다. 하지만 Amazon CloudWatch 경보를 생성하고 준비 상태 검사를 생성하여 경보 상태를 모니터링할 수 있습니다. 예를 들어 Amazon EKS 컨테이너 서비스를 모니터링하는 사용자 지정 CloudWatch 경보를 생성하고 경보의 준비 상태를 감사하기 위한 준비 검사를 생성할 수 있습니다.

리소스 세트를 생성할 AWS Management Console 때 에서 각 리소스 유형에 대한 모든 준비 규칙을 보거나 나중에 리소스 세트의 세부 정보 페이지로 이동하여 준비 규칙을 볼 수 있습니다. 다음 섹션에서 준비 규칙을 볼 수도 있습니다. Route 53 ARC의 준비 규칙

준비 확인을 통해 일련의 규칙을 사용하여 리소스 세트를 감사하는 경우 각 규칙이 정의되는 방식에 따라 결과가 모든 리소스의 `READY` 또는 `NOT READY`에 적용될지 아니면 리소스별로 결과가 달라질지 여부가 결정됩니다. 또한 다양한 방법으로 준비 확인을 볼 수 있습니다. 예를 들어, 리소스 세트에 있는 리소스 그룹의 준비 상태를 보거나 복구 그룹 또는 셀 (즉, 복구 그룹 설정 방법에 따라 AWS 지역 또는 가용 영역) 의 준비 상태 요약을 볼 수 있습니다.

각 규칙 설명의 문구에는 해당 규칙이 적용될 때 리소스를 평가하여 준비 상태를 결정하는 방법이 설명되어 있습니다. 규칙은 각 리소스를 검사하거나 리소스 세트의 모든 리소스를 검사하여 준비를 판단하도록 정의됩니다. 구체적으로, 규칙은 다음과 같이 작동합니다.

- 규칙은 리소스 세트의 각 리소스를 검사하여 조건을 확인합니다.

  - 모든 리소스가 성공하면 모든 리소스가 READY로 설정됩니다.
  - 한 리소스에 장애가 발생하면 해당 리소스는 NOT READY로 설정되고 다른 셀은 READY로 유지됩니다.

  예를 들어 MskClusterState:는 각 Amazon MSK 클러스터를 검사하여 ACTIVE 상태가 정상인지 확인합니다.
- 규칙은 리소스 세트의 모든 리소스를 검사하여 조건을 확인합니다.
  - 조건이 보장되면 모든 리소스가 READY로 설정됩니다.
  - 조건을 충족하지 못하는 경우 모든 리소스가 NOT READY로 설정됩니다.

  예를 들어 VpcSubnetCount:는 모든 VPC 서브넷을 검사하여 서브넷 수가 같은지 확인합니다.
- 중요하지 않은 규칙: 규칙은 리소스 세트의 모든 리소스를 검사하여 조건을 확인합니다.
  - 실패하더라도 준비 상태는 변경되지 않습니다. 이 동작이 있는 규칙의 설명에는 메모가 있습니다.

  예를 들어 ElbV2CheckAzCount:는 각 Network Load Balancer를 검사하여 하나의 가용 영역에만 연결되어 있는지 확인합니다. 참고: 이 규칙은 준비 상태에는 영향을 미치지 않습니다.

또한 Route 53 ARC는 할당량을 위한 추가 조치를 취합니다. 준비 확인에서 지원되는 리소스의 Service Quotas(리소스 생성 및 운영의 최대값)에 대한 셀 간의 불일치가 감지되면 Route 53 ARC는 할당량이 낮은 리소스의 할당량을 자동으로 올립니다. 이는 할당량(제한)에만 적용됩니다. 용량을 확보하려면 애플리케이션 요구 사항에 따라 필요한 대로 용량을 추가해야 합니다.

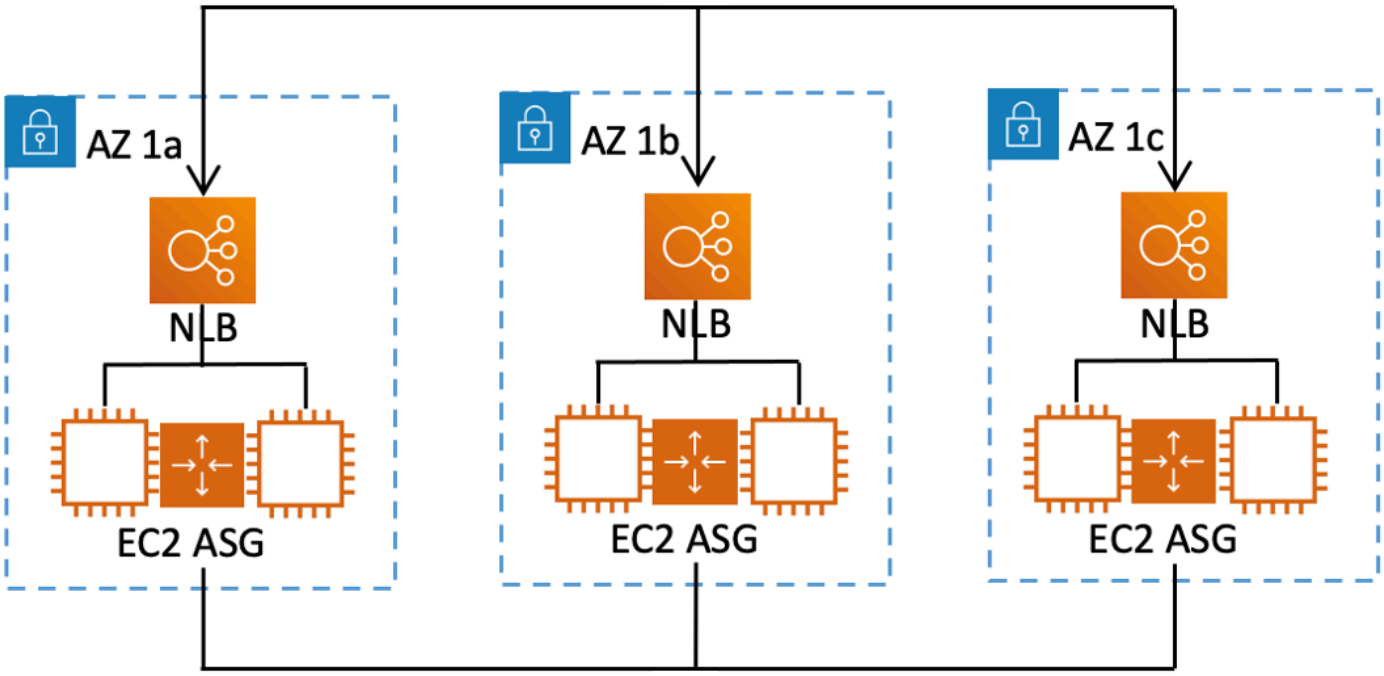
준비 확인 (예: 준비 확인 상태가 로 변경될 때) 을 위한 Amazon EventBridge 알림을 설정할 수도 있습니다. NOT READY 그런 다음 구성 불일치가 감지되면 알림을 EventBridge 보내며 애플리케이션 복제본이 정렬되고 복구에 대비할 수 있도록 시정 조치를 취할 수 있습니다. 자세한 정보는 Amazon에서 Route 53 ARC에서 준비 상태 확인 사용하기 EventBridge을 참조하세요.

준비 검사, 리소스 세트 및 준비 범위가 함께 작동하는 방식

준비 검사는 항상 리소스 세트의 리소스 그룹을 감사합니다. 리소스 세트를 별도로 또는 준비 검사를 생성하는 동안 Route 53 ARC 복구 그룹의 셀 (가용 영역 또는 AWS 지역) 에 있는 리소스를 그룹화하여 준비 검사를 정의할 수 있습니다. 리소스 세트는 일반적으로 동일한 유형의 리소스(예: Network Load Balancer)의 그룹이지만 아키텍처 준비 확인을 위한 DNS 대상 리소스일 수도 있습니다.

일반적으로 하나의 리소스 세트를 만들고 애플리케이션의 각 리소스 유형에 대해 준비 확인을 수행합니다. 아키텍처 준비 확인의 경우 최상위 DNS 대상 리소스와 이에 대한 글로벌(복구 그룹 수준) 리소스 세트를 만든 다음 별도의 리소스 세트에 대한 셀 수준 DNS 대상 리소스를 만듭니다.

다음 다이어그램은 각각 Network Load Balancer(NLB) 및 오토 스케일링(ASG)이 있는 세 개의 셀(가용 영역)로 구성된 복구 그룹의 예를 보여줍니다.



이 시나리오에서는 세 개의 Network Load Balancer에 대한 리소스 세트와 준비 확인을 생성하고, 세 개의 오토 스케일링에 대한 리소스 세트와 준비 확인을 생성합니다. 이제 복구 그룹의 각 리소스 세트를 리소스 유형별로 준비했는지 확인할 수 있습니다.

리소스에 대한 준비 범위를 생성하여 셀 또는 복구 그룹에 대한 준비 확인 요약을 추가할 수 있습니다. 리소스의 준비 범위를 지정하려면 셀 또는 복구 그룹의 ARN을 리소스 세트의 각 리소스에 연결합니다. 이 작업은 리소스 세트에 대한 준비 확인을 생성할 때 수행할 수 있습니다.

예를 들어 이 복구 그룹의 Network Load Balancer 리소스 세트에 대한 준비 확인을 추가할 때 각 NLB에 준비 범위를 동시에 추가할 수 있습니다. 이 경우 AZ 1a의 ARN을 AZ 1a의 NLB에 연결하고, AZ 1b의 ARN을 NLB AZ 1b에 연결하고, AZ 1c의 ARN을 AZ 1c의 NLB에 연결합니다. 오토 스케일링에 대한 준비 확인을 생성할 때는 오토 스케일링 리소스 세트에 대한 준비 확인을 생성할 때 각 그룹에 준비 범위를 할당하여 동일한 작업을 수행합니다.

준비 확인을 생성할 때 준비 범위를 연결하는 것은 선택 사항이지만 준비 범위를 설정하는 것이 좋습니다. 준비 범위를 사용하면 Route 53 ARC가 복구 그룹 요약 준비 확인 및 셀 수준 요약 준비 확인에 대한 올바른 READY 또는 NOT READY 준비 상태를 표시할 수 있습니다. 준비 범위를 설정하지 않는 한 Route 53 ARC는 이러한 요약을 제공할 수 없습니다.

애플리케이션 수준 또는 글로벌 리소스(예: DNS 라우팅 정책)를 추가할 때는 준비 범위로 복구 그룹이나 셀을 선택하지 않는다는 점에 유의하십시오. 대신 글로벌 리소스(셀 없음)를 선택합니다.

DNS 대상 리소스 준비 확인: 복원력 준비 감사

Route 53 ARC의 DNS 대상 리소스 준비 검사를 사용하면 애플리케이션의 아키텍처 및 복원력 준비 상태를 감사할 수 있습니다. 이러한 유형의 준비 확인은 애플리케이션의 아키텍처와 Amazon Route 53 라우팅 정책을 지속적으로 스캔하여 영역 간 및 리전 간 종속성을 감사합니다.

복구 지향 애플리케이션에는 가용 영역 또는 AWS 지역에 사일로된 여러 복제본이 있으므로 복제본이 서로 독립적으로 실패할 수 있습니다. 애플리케이션이 올바르게 사일로화되도록 조정해야 하는 경우 Route 53 ARC는 필요한 경우 아키텍처를 업데이트하여 복원력이 뛰어나고 장애 조치에 대비할 수 있도록 변경할 수 있는 사항을 제안합니다.

Route 53 ARC는 애플리케이션의 셀 수 및 범위(복제본 또는 장애 억제 유닛), 셀이 가용 영역별로 또는 리전별로 격리되어 있는지 여부를 자동으로 감지합니다. 그런 다음 Route 53 ARC는 셀의 애플리케이션 리소스에 대한 정보를 식별하고 제공하여 해당 리소스가 영역 또는 리전에 올바르게 사일로되어 있는지 확인합니다. 예를 들어, 특정 영역으로 범위가 지정된 셀이 있는 경우, 준비 확인을 통해 로드 밸런서와 그 뒤에 있는 대상도 해당 영역으로 격리되어 있는지 모니터링할 수 있습니다.

이 정보를 사용하여 셀의 리소스를 올바른 영역 또는 리전에 맞추기 위해 변경해야 할 사항이 있는지 확인할 수 있습니다.

시작하려면 애플리케이션의 DNS 대상 리소스와 이에 대한 리소스 세트 및 준비 확인을 생성해야 합니다. 자세한 정보는 Route 53 ARC에서 아키텍처 권장 사항 확인하기을 참조하세요.

준비 확인 및 재해 복구 시나리오

Route 53 ARC 준비 검사를 통해 애플리케이션이 장애 조치 트래픽을 처리할 수 있도록 확장되었는지 확인할 수 있으므로 애플리케이션과 리소스가 복구 준비가 되었는지 여부를 파악할 수 있습니다. 준비 확인을 프로덕션 복제본이 정상임을 나타내는 신호로 사용해서는 안 됩니다. 그러나 애플리케이션 및 인프라 모니터링 또는 상태 확인 시스템 대신 준비 확인을 사용하여 복제본에 대한 장애 조치 여부를 결정할 수 있습니다.

긴급 상황이나 운영 중단이 발생하는 경우 상태 확인과 기타 정보를 조합하여 대기 복제본이 확장되고 정상 상태이며 프로덕션 트래픽의 장애 조치에 대비할 준비가 되었는지 확인합니다. 예를 들어 대기 셀에서 실행되는 canary가 성공 기준을 충족하는지 확인하고 대기 셀의 준비 확인 상태가 READY인지 확인합니다.

Route 53 ARC 준비 확인은 미국 서부(오레곤)의 단일 AWS 리전에서 호스팅되므로 운영 중단 또는 재해 발생 시 준비 확인 정보가 유효하지 않거나 확인을 사용할 수 없게 될 수 있다는 점에 유의하세요. 자세한 정보는 라우팅 제어를 위한 데이터 및 컨트롤 플레인을 참조하세요.

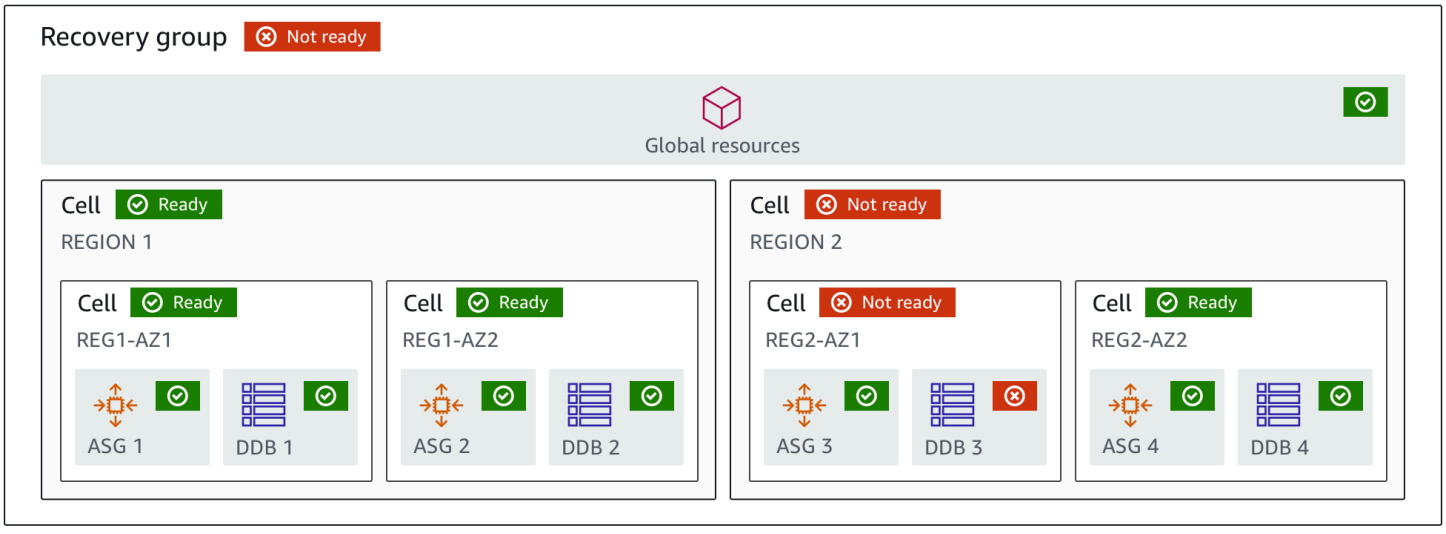
AWS 준비 상태 확인을 위한 지역 가용성

Amazon Route 53 Application Recovery Controller의 리전 지원 및 서비스 엔드포인트에 대한 자세한 내용은 Amazon Web Services 일반 참조의 Amazon Route 53 Application Recovery Controller 엔드포인트 및 할당량을 참조하세요.

> **Note**
>
> Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인은 글로벌 기능입니다. 하지만 준비 확인 리소스는 미국 서부 (오레곤) 지역에 있으므로 Regional Route 53 ARC AWS CLI 명령에서 미국 서부 (오레곤) 지역을 지정 (파라미터 지정`--region us-west-2`) 해야 합니다 (예: 리소스 세트 및 준비 확인과 같은 리소스를 생성할 때).

준비 확인 구성 요소

다음 다이어그램은 준비 확인 기능을 지원하도록 구성된 샘플 복구 그룹을 보여줍니다. 이 예제의 리소스는 복구 그룹에서 셀 (기준 AWS 리전) 과 중첩된 셀 (가용 영역별) 으로 그룹화됩니다. 복구 그룹(애플리케이션)의 전반적인 준비 상태는 물론 각 셀(리전) 및 중첩된 셀(가용 영역)에 대한 개별 준비 상태도 있습니다.



Route 53 ARC의 준비 확인 기능의 구성 요소는 다음과 같습니다.

셀

셀은 애플리케이션의 복제본 또는 독립된 장애 조치 단위를 정의합니다. 복제본 내에서 애플리케이션을 독립적으로 실행하는 데 필요한 모든 AWS 리소스를 그룹화합니다. 예를 들어 기본 셀에는 리소스 세트 하나가 있고 대기 셀에는 다른 리소스 세트가 있을 수 있습니다. 셀에 포함되는 항목의 경계는 사용자가 결정하지만 셀은 일반적으로 가용 영역 또는 리전을 나타냅니다. 리전 내의 AZ와 같이 셀 내에 여러 셀(중첩된 셀)이 있을 수 있습니다. 각 중첩된 셀은 격리된 장애 조치 단위를 나타냅니다.

복구 그룹

셀은 복구 그룹으로 수집됩니다. 복구 그룹은 장애 조치 준비를 확인할 애플리케이션 또는 애플리케이션 그룹을 나타냅니다. 기능면에서 서로 일치하는 두 개 이상의 셀 또는 복제본으로 구성됩니다. 예를 들어 us-east-1a 및 us-east-1b(us-east-1b)를 통해 복제되는 웹 애플리케이션이 있는 경우, 여기서 us-east-1b는 장애 조치 환경이며 Route 53 ARC에서 이 애플리케이션을 us-east-1a에 있는 셀과 us-east-1b의 셀로 구성된 복구 그룹으로 표현할 수 있습니다. 복구 그룹에는 Route 53 상태 확인과 같은 글로벌 리소스도 포함될 수 있습니다.

리소스 및 리소스 식별자

Route 53 ARC에서 준비 확인을 위한 구성 요소를 생성할 때는 리소스 식별자를 사용하여 Amazon DynamoDB 테이블, Network Load Balancer 또는 DNS 대상 리소스와 같은 리소스를 지정합니다. 리소스 식별자는 리소스의 Amazon 리소스 이름(ARN)이거나, DNS 대상 리소스의 경우 Route 53 ARC가 리소스를 생성할 때 생성하는 식별자입니다.

DNS 대상 리소스

DNS 대상 리소스는 애플리케이션의 도메인 이름과 도메인이 가리키는 AWS 리소스와 같은 기타 DNS 정보의 조합입니다. AWS 리소스 포함은 선택 사항이지만 제공하는 경우 이는 Route 53 리소스 레코드 또는 Network Load Balancer여야 합니다. AWS 리소스를 제공하면 애플리케이션의 복구 복원력을 개선하는 데 도움이 될 수 있는 보다 자세한 아키텍처 권장 사항을 얻을 수 있습니다. Route 53 ARC에서 DNS 대상 리소스용 리소스 세트를 생성한 다음, 리소스 세트에 대한 준비 확인을 생성하여 애플리케이션에 대한 아키텍처 권장 사항을 얻을 수 있습니다. 또한 준비 확인은 DNS 대상 리소스에 대한 준비 규칙을 기반으로 애플리케이션의 DNS 라우팅 정책을 모니터링합니다.

리소스 세트

리소스 세트는 리소스 또는 DNS 대상 AWS 리소스를 포함하여 여러 셀에 걸쳐 있는 리소스 집합입니다. 예를 들어 us-east-1a에 로드 밸런서가 있고 us-east-1b에 로드 밸런서가 하나 있을 수 있습니다. 로드 밸런서의 복구 준비를 모니터링하려면 두 로드 밸런서를 모두 포함하는 리소스 세트를 만든 다음 리소스 세트에 대한 준비 확인을 생성하면 됩니다. Route 53 ARC는 세트에 있는 리소스의

준비를 지속적으로 확인합니다. 준비 범위를 추가하여 리소스 세트의 리소스를 애플리케이션용으로 생성한 복구 그룹과 연결할 수도 있습니다.

준비 규칙

준비 규칙은 Route 53 ARC가 리소스 세트의 리소스 세트에 대해 수행하는 감사입니다. Route 53 ARC에는 준비 확인을 지원하는 각 리소스 유형에 대한 준비 규칙 세트가 있습니다. 각 규칙에는 Route 53 ARC가 리소스를 검사하는 대상을 설명하는 ID와 설명이 포함되어 있습니다.

준비 확인

준비 확인은 Route 53 ARC가 복구 준비를 감사하는 Amazon Aurora 인스턴스 세트와 같은 애플리케이션의 리소스 세트를 모니터링합니다. 준비 확인에는 용량 구성, AWS 할당량 또는 라우팅 정책과 같은 감사가 포함될 수 있습니다. 예를 들어, 두 가용 영역에 걸친 Amazon EC2 Auto Scaling 그룹의 준비를 감사하려는 경우, 오토 스케일링당 하나씩, 두 개의 리소스 ARN이 있는 리소스 세트에 대한 준비 확인을 생성할 수 있습니다. 그런 다음 각 그룹이 동일하게 확장되도록 Route 53 ARC는 두 그룹의 인스턴스 유형과 개수를 지속적으로 모니터링합니다.

준비 범위

준비 범위는 특정 준비 확인에 포함되는 리소스 그룹을 식별합니다. 준비 확인의 범위는 복구 그룹(즉, 전체 애플리케이션에 대한 전역) 또는 셀(즉, 리전 또는 가용 영역)일 수 있습니다. Route 53 ARC의 글로벌 리소스인 리소스의 경우 준비 범위를 복구 그룹 또는 글로벌 리소스 수준으로 설정합니다. 예를 들어, Route 53 상태 확인은 리전이나 가용 영역에만 국한되지 않기 때문에 Route 53 ARC의 글로벌 리소스에 해당합니다.

준비 상태 점검을 위한 데이터 및 컨트롤 플레인

페일오버와 재해 복구를 계획할 때는 페일오버 메커니즘이 얼마나 탄력적인지 생각해 보세요. 재해 시나리오에서 필요할 때 사용할 수 있도록 페일오버 중에 사용하는 메커니즘의 가용성이 높은지 확인하는 것이 좋습니다. 일반적으로 안정성과 내결함성을 극대화하려면 가능하면 언제든지 메커니즘에 데이터 플레인 함수를 사용해야 합니다. 이를 염두에 두고 서비스의 기능이 컨트롤 플레인과 데이터 영역 간에 어떻게 구분되는지, 그리고 서비스의 데이터 영역에서 최상의 신뢰성을 기대할 수 있는 경우를 이해하는 것이 중요합니다.

대부분의 AWS 서비스와 마찬가지로 준비 상태 검사 기능에 대한 기능은 컨트롤 플레인 및 데이터 플레인에서 지원됩니다. 둘 다 신뢰성을 위해 구축되었지만 컨트롤 플레인은 데이터 일관성을 위해 최적화되고 데이터 플레인은 가용성을 위해 최적화됩니다. 데이터 영역은 복원력을 고려하여 설계되었으므로 컨트롤 플레인 사용이 불가능해질 수 있는 운영 중단에도 가용성을 유지할 수 있습니다.

일반적으로 컨트롤 플레인을 사용하면 서비스의 리소스 생성, 업데이트 및 삭제와 같은 기본 관리 기능을 수행할 수 있습니다. 데이터 영역은 서비스의 핵심 기능을 제공합니다.

준비 상태 확인을 위해 컨트롤 플레인과 데이터 플레인 모두에 대해 복구 준비 API라는 단일 API가 있습니다. 준비 확인 및 준비 리소스는 미국 서부(오레곤) 리전(us-west-2)에만 있습니다. 준비 상태 검사 컨트롤 플레인과 데이터 플레인은 신뢰할 수 있지만 가용성이 높지는 않습니다.

데이터 플레인, 컨트롤 플레인, 고가용성 목표를 달성하기 위해 서비스를 AWS 구축하는 방법에 대한 자세한 내용은 Amazon Builders' Library의 가용 영역을 사용한 정적 안정성 문서를 참조하십시오.

Amazon Route 53 애플리케이션 복구 컨트롤러에서의 준비 상태 확인을 위한 태깅

태그는 리소스를 식별하고 구성하는 데 사용하는 단어 또는 문구 (메타데이터) 입니다. AWS 각 리소스에 태그를 여러 개 추가할 수 있고, 각 태그는 사용자가 정의한 키와 값을 포함할 수 있습니다. 예를 들어, 키는 환경이고 값은 생산일 수 있습니다. 추가하는 태그에 따라 리소스를 검색하고 필터링할 수 있습니다.

Route 53 ARC에서 준비 상태 확인 시 다음 리소스에 태그를 지정할 수 있습니다.

- 리소스 세트
- 준비 확인

Route 53 ARC에서의 태그 지정은 API를 통해서만 사용할 수 있습니다(예: AWS CLI사용).

다음은 를 사용하여 준비 상태 확인에 태그를 지정하는 예입니다. 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
```

자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러용 복구 준비 API 참조 안내서를 참조하십시오 TagResource.

Route 53 ARC에서의 준비 상태 확인 요금

Amazon Route 53 Application Recovery Controller를 사용하면 서비스에서 사용하도록 구성한 만큼만 비용을 지불하면 됩니다. 준비 상태 확인의 경우 구성한 준비 검사당 시간당 비용을 지불합니다.

Route 53 ARC에 대한 자세한 요금 정보와 요금 예제를 보려면 Amazon Route 53 애플리케이션 복구 컨트롤러 요금을 참조하고 Amazon Route 53 애플리케이션 복구 컨트롤러로 스크롤을 내리십시오.

애플리케이션에 대한 복원력 있는 복구 프로세스를 설정하십시오.

여러 AWS 지역에 있는 AWS 애플리케이션에서 Amazon Route 53 애플리케이션 복구 컨트롤러를 사용하려면 복구 준비를 효과적으로 지원할 수 있도록 애플리케이션을 복원력을 갖추도록 설정하는 데 따라야 할 지침이 있습니다. 그런 다음 애플리케이션에 대한 준비 검사를 생성하고 장애 조치를 위해 트래픽을 다시 라우팅하도록 라우팅 제어를 설정할 수 있습니다. 또한 복원력을 개선할 수 있는 애플리케이션 아키텍처에 대해 Route 53 ARC가 제공하는 권장 사항을 검토할 수 있습니다.

> **Note**
>
> 가용 영역에 의해 격리된 애플리케이션이 있는 경우 장애 조치 복구를 위해 영역 이동 또는 영역 자동 이동을 사용하는 것을 고려해 보십시오. 가용 영역 장애로부터 애플리케이션을 안정적으로 복구하기 위해 영역 이동 또는 영역 자동 이동을 사용하기 위한 설정은 필요하지 않습니다.
>
> 로드 밸런서 리소스의 가용 영역에서 트래픽을 다른 곳으로 이동하려면 Route 53 ARC 콘솔 또는 Elastic Load Balancing 콘솔에서 영역 이동을 시작하십시오. AWS Command Line Interface 또는 AWS SDK를 영역 이동 API 작업과 함께 사용할 수도 있습니다. 자세한 정보는 Amazon Route 53 Application Recovery Controller의 영역 전환을 참조하세요.

복원력 있는 페일오버 구성을 시작하는 방법에 대한 자세한 내용은 을 참조하십시오. Amazon Route 53 Application Recovery Controller의 다중 리전 복구 시작하기

Route 53 ARC에서의 준비 상태 확인에 대한 모범 사례

Amazon Route 53 애플리케이션 복구 컨트롤러에서 준비 상태를 확인할 수 있도록 다음 모범 사례를 사용하는 것이 좋습니다.

준비 상태 변경에 대한 알림 추가

Amazon에서 준비 확인 상태가 변경될 때마다 알림을 EventBridge 보내도록 규칙을 설정합니다 (예: 에서 READY 로NOT READY). 알림을 받으면 문제를 조사하고 해결하여 애플리케이션과 리소스가 예상한 시기에 장애 조치를 수행할 준비가 되었는지 확인할 수 있습니다.

복구 그룹 (애플리케이션용), 셀 (예: AWS 지역) 또는 리소스 세트의 준비 확인 등 여러 준비 상태 확인 상태 변경에 대해 알림을 전송하도록 EventBridge 규칙을 설정할 수 있습니다.

자세한 정보는 Amazon에서 Route 53 ARC에서 준비 상태 확인 사용하기 EventBridge을 참조하세요.

준비 검사 API 작업

다음 표에는 복구 준비 상태(준비 상태 확인)에 사용할 수 있는 Route 53 ARC 작업이 관련 설명서 링크와 함께 나열되어 있습니다.

AWS Command Line Interface에서 일반적인 복구 준비 상태 API 작업을 사용하는 방법에 대한 예는 Route 53 ARC 준비 상태 확인 API 작업을 다음과 함께 사용하는 예 AWS CLI 섹션을 참조하세요.

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
셀 생성	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	참조 CreateCell
셀 가져오기	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	참조 GetCell
셀 삭제	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	참조 DeleteCell
셀 업데이트	N/A	참조 UpdateCell
계정의 셀 목록	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	참조 ListCells
복구 그룹 생성	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	CreateRecovery그룹 참조
복구 그룹 가져오기	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	GetRecovery그룹 참조

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
복구 그룹 생성	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	UpdateRecovery그룹 참조
복구 그룹 삭제	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	DeleteRecovery그룹 참조
복구 그룹 나열	Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제 섹션 참조	ListRecovery그룹 참조
리소스 세트 생성	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	CreateResource세트 참조
리소스 세트 가져오기	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	GetResource세트 참조
리소스 세트 업데이트	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	UpdateResource세트 참조
리소스 세트 삭제	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	DeleteResource세트 참조
리소스 세트 나열	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	ListResource세트 참조
준비 확인 생성	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	CreateReadiness체크 참조
준비 확인 가져오기	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	GetReadiness체크 참조
준비 확인 업데이트	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	UpdateReadiness체크 참조
준비 확인 삭제	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	DeleteReadiness체크 참조
준비 확인 나열	Route 53 ARC에서 준비 확인 생성 및 업데이트 섹션 참조	ListReadiness수표 참조

작업	Route 53 ARC 콘솔 사용	Route 53 ARC API 사용
준비 규칙 나열	Route 53 ARC의 준비 규칙 설명 섹션 참조	참조 ListRules
전체 준비 확인 상태 점검	Route 53 ARC에서의 준비 확인 모니터링 섹션 참조	참조 GetReadinessCheckStatus
리소스 상태 확인	Route 53 ARC에서의 준비 확인 모니터링 섹션 참조	GetReadinessCheckResource 상태 참조
셀 상태 확인	Route 53 ARC에서의 준비 확인 모니터링 섹션 참조	참조 GetCellReadinessSummary
복구 그룹 상태 확인	Route 53 ARC에서의 준비 확인 모니터링 섹션 참조	GetRecoveryGroupReadiness 요약 참조

Route 53 ARC 준비 상태 확인 API 작업을 다음과 함께 사용하는 예 AWS CLI

이 섹션에서는 API 작업을 AWS Command Line Interface 사용하여 Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인 기능을 사용하는 간단한 애플리케이션 예제를 살펴봅니다. 이 예제는 CLI를 사용하여 준비 상태 검사 기능을 사용하는 방법에 대한 기본적인 이해를 돕기 위한 것입니다.

Route 53 ARC의 준비 상태 검사는 애플리케이션 복제본의 리소스 불일치를 감사합니다. 애플리케이션에 대한 준비 검사를 설정하려면 애플리케이션용으로 생성한 복제본에 맞춰 Route 53 ARC 셀에서 애플리케이션 리소스를 설정 또는 모델링해야 합니다. 그런 다음 이러한 복제본을 감사하는 준비 검사를 설정하여 대기 애플리케이션 복제본과 해당 리소스가 프로덕션 복제본과 일치하는지 지속적으로 확인할 수 있습니다.

현재 미국 동부(버지니아 북부) 리전(us-east-1)에서 실행되는 Simple-Service 애플리케이션이 있는 간단한 경우를 살펴보겠습니다. 또한 미국 서부(오레곤) 리전(us-west-2)에 애플리케이션의 대기 복사본이 있습니다. 이 예시에서는 두 버전의 애플리케이션을 비교하도록 준비 확인을 구성해 보겠습니다. 이를 통해 장애 조치 시나리오에서 필요한 경우 대기 중인 미국 서부(오레곤) 리전에서 트래픽을 수신할 준비가 되었는지 확인할 수 있습니다.

사용에 대한 자세한 내용은 명령 AWS CLI참조를 참조하십시오.AWS CLI 준비 상태 API 작업 목록 및 자세한 정보 링크는 준비 검사 API 작업 섹션을 참조하세요.

Route 53 ARC의 셀은 장애 경계(예: 가용 영역 또는 리전)를 나타내며 복구 그룹으로 수집됩니다. 복구 그룹은 장애 조치 준비를 확인하려는 애플리케이션을 나타냅니다. 준비 상태 확인 구성 요소에 대한 자세한 내용은 준비 확인 구성 요소 섹션을 참조하세요.

> **Note**
>
> Route 53 ARC는 여러 엔드포인트를 지원하는 글로벌 AWS 리전 서비스이지만 대부분의 Route 53 ARC CLI 명령에서 미국 서부 (오레곤) 지역을 지정 (즉, 파라미터 지정`--region us-west-2`) 해야 합니다. 예를 들어 복구 그룹 또는 준비 확인과 같은 리소스를 생성할 수 있습니다.

애플리케이션 예제에서는 먼저 리소스가 있는 각 리전에 대해 하나의 셀을 생성해 보겠습니다. 그런 다음 복구 그룹을 만든 후 준비 확인을 위한 설정을 완료합니다.

1. 셀 생성

1a. us-east-1 셀을 생성합니다.

```
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. us-east-1 셀을 생성합니다.

```
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. 이제 두 셀이 생겼습니다. `list-cells` API를 호출하여 이들이 존재하는지 확인할 수 있습니다.

```
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. 복구 그룹 생성

복구 그룹은 Route 53 ARC의 복구 준비를 위한 최상위 리소스입니다. 복구 그룹은 애플리케이션 전체를 나타냅니다. 이 단계에서는 전체 애플리케이션을 모델링하는 복구 그룹을 만든 다음 앞서 만든 두 개의 셀을 추가합니다.

2a. 복구 그룹을 생성합니다.

```
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. (선택 사항) `list-recovery-groups` API를 호출하여 복구 그룹이 올바르게 생성되었는지 확인할 수 있습니다.

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

이제 애플리케이션 모델을 만들었으니 모니터링할 리소스를 추가해 보겠습니다. Route 53 ARC에서는 모니터링하려는 리소스 그룹을 리소스 세트라고 합니다. 리소스 세트에는 모두 같은 유형의 리소스가 포함되어 있습니다. 리소스 세트의 리소스를 서로 비교하여 셀의 장애 조치 준비 상태를 판단할 수 있습니다.

3. 리소스 세트 생성

Simple-Service 애플리케이션이 정말 간단하고 DynamoDB 테이블만 사용한다고 가정해 보겠습니다. us-east-1에 DynamoDB 테이블이 있고 us-west-2에 또 다른 테이블이 있습니다. 리소스 세트에는 각 리소스가 포함된 셀을 식별하는 준비 범위도 포함되어 있습니다.

3a. Simple-Service 애플리케이션의 리소스를 반영하는 리소스 세트를 생성합니다.

```
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. (선택 사항) `list-resource-sets` API를 호출하여 리소스 세트에 무엇이 포함되어 있는지 확인할 수 있습니다. 여기에는 AWS 계정의 모든 리소스 세트가 나열됩니다. 여기서 위에서 만든 리소스 세트가 하나뿐임을 알 수 있습니다.

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

이제 Route 53 ARC에서 Simple-Service 애플리케이션을 모델링하기 위한 셀, 복구 그룹, 리소스 세트를 생성했습니다. 다음으로, 리소스의 장애 조치 준비를 모니터링하기 위한 준비 확인을 설정해 보겠습니다.

4. 준비 확인 생성

준비 확인은 확인에 연결된 리소스 세트의 각 리소스에 규칙 세트를 적용합니다. 규칙은 각 리소스 유형별로 다릅니다. 즉, `AWS::DynamoDB::Table`, `AWS::EC2::Instance` 등에 대한 다양한 규칙이 있습니다. 규칙은 구성, 용량(사용 가능하고 해당하는 경우), 제한(사용 가능하고 해당하는 경우), 라우팅 구성 등 리소스의 다양한 차원을 확인합니다.

> **Note**
>
> 준비 확인에서 리소스에 적용되는 규칙을 보기 위해 5단계에서 설명한 대로 `get-readiness-check-resource-status` API를 사용할 수 있습니다. Route 53 ARC의 모든 준비 규칙 목록을 보려면 `list-rules`를 사용하거나 Route 53 ARC의 준비 규칙 설명 섹션을 참조하세요. Route 53 ARC에는 각 리소스 유형에 대해 실행하는 특정 규칙 세트가 있으며, 현재로서는 사용자 지정할 수 없습니다.

4a. 리소스 세트 ImportantInformationTables에 대한 준비 확인을 생성합니다.

```
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. (선택 사항) 준비 확인이 성공적으로 생성되었는지 확인하려면 `list-readiness-checks` API를 실행합니다. 이 API는 계정의 모든 준비 확인을 보여줍니다.

```
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. 준비 확인 모니터링

애플리케이션을 모델링하고 준비 확인을 추가했으니 이제 리소스를 모니터링할 준비가 되었습니다. 준비 확인 수준(리소스 그룹), 개별 리소스 수준, 셀 수준(가용 영역 또는 리전의 모든 리소스), 복구 그룹 수준(전체 애플리케이션)의 4가지 수준에서 애플리케이션의 준비를 모델링할 수 있습니다. 이러한 각 유형의 준비 상태를 가져오는 명령이 아래에 나와 있습니다.

5a. 준비 확인 상태를 확인합니다.

```
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. 확인되는 각 규칙의 상태를 포함하여 준비 확인에서 단일 리소스의 자세한 준비 상태를 확인할 수 있습니다.

```
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. 셀의 전반적인 준비 상태를 확인합니다.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary \
    --cell-name west-cell
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

5d. 마지막으로 복구 그룹 수준에서 애플리케이션의 최상위 준비를 확인합니다.

```
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"
        }
    ]
}
```

복구 그룹 및 준비 확인 관련 작업

이 섹션에서는 이러한 리소스의 생성, 업데이트 및 삭제를 포함하여 복구 그룹 및 준비 상태 검사에 대한 절차를 설명하고 제공합니다.

Route 53 ARC에서 복구 그룹 생성, 업데이트, 삭제

복구 그룹은 Amazon Route 53 Application Recovery Controller의 애플리케이션을 나타냅니다. 일반적으로 리소스와 기능 측면에서 서로 복제된 둘 이상의 셀로 구성되므로 한 셀에서 다른 셀로 장애 조치할 수 있습니다. 각 셀에는 한 AWS 지역 또는 가용 영역의 활성 리소스에 대한 Amazon 리소스 이름

(ARN) 이 포함됩니다. 리소스는 Elastic Load Balcing 로드 밸런서, 오토 스케일링 또는 기타 리소스일 수 있습니다. 다른 영역 또는 리전을 나타내는 해당 셀에는 활성 셀에 있는 동일한 유형의 대기 리소스(로드 밸런서, 오토 스케일링 등)가 있습니다.

셀은 애플리케이션의 복제본을 나타냅니다. Route 53 ARC의 준비 확인을 통해 애플리케이션이 한 복제본에서 다른 복제본으로 장애 조치할 준비가 되었는지 확인할 수 있습니다. 하지만 모니터링 및 상태 확인 시스템을 기반으로 복제본에서 장애 조치를 취할지 아니면 복제본으로 장애 조치할지 결정해야 하며, 이러한 시스템에 대한 보완 서비스로서 준비 확인을 고려해야 합니다.

준비 확인은 리소스를 감사하여 해당 리소스 유형에 대해 미리 정의된 규칙 세트를 기반으로 준비 확인을 결정합니다. 복제본으로 복구 그룹을 생성한 후 애플리케이션의 리소스에 대한 Route 53 ARC 준비 확인을 추가하여 시간이 지나도 복제본이 동일한 설정 및 구성을 유지하도록 Route 53 ARC를 통해 확인할 수 있습니다.

주제

복구 그룹 생성

이 섹션의 단계에서는 Route 53 ARC 콘솔에서 복구 그룹을 생성하는 방법을 설명합니다. Amazon Route 53 Application Recovery Controller에서 복구 준비 API 작업을 사용하는 방법을 보려면 준비 검사 API 작업 섹션을 참조하세요.

복구 그룹 생성

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 준비 확인을 선택합니다.
3. 복구 준비 페이지에서 생성을 선택한 다음 복구 그룹을 선택합니다.
4. 복구 그룹의 이름을 입력하고 다음을 선택합니다.
5. 셀 생성을 선택하고 셀 추가를 선택합니다.
6. 셀 이름을 입력합니다. 예를 들어 미국 서부(캘리포니아 북부)에 애플리케이션 복제본이 있는 경우 `MyApp-us-west-1` 이름이 지정된 셀을 추가할 수 있습니다.
7. 셀 추가를 선택하고 두 번째 셀의 이름을 추가합니다. 예를 들어 미국 동부(오하이오)에 복제본이 있는 경우 `MyApp-us-east-2` 이름이 지정된 셀을 추가할 수 있습니다.

8. 중첩된 셀(리전 내 가용 영역에 있는 복제본)을 추가하려면 작업을 선택하고 중첩 셀 추가를 선택한 다음 이름을 입력합니다.
9. 애플리케이션 복제본의 모든 셀과 중첩 셀을 추가했으면 다음을 선택합니다.
10. 복구 그룹을 검토한 다음 복구 그룹 생성을 선택합니다.

복구 그룹과 셀 업데이트 및 삭제

이 섹션의 단계에서는 Route 53 ARC 콘솔에서 복구 그룹을 업데이트 및 삭제하고 셀을 삭제하는 방법에 대해 설명합니다. Amazon Route 53 Application Recovery Controller에서 복구 준비 API 작업을 사용하는 방법을 보려면 준비 검사 API 작업 섹션을 참조하세요.

복구 그룹을 업데이트 또는 삭제, 셀 삭제

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 준비 확인을 선택합니다.
3. 복구 준비 페이지에서 복구 그룹을 선택합니다.
4. 복구 그룹 작업을 수행하려면 작업을 선택한 다음 복구 그룹 편집 또는 복구 그룹 삭제를 선택합니다.
5. 복구 그룹을 편집할 때 셀 또는 중첩된 셀을 추가하거나 제거할 수 있습니다.
   - 셀을 추가하려면 셀 추가를 선택합니다.
   - 셀을 제거하려면 셀 옆의 작업 레이블에서 셀 삭제를 선택합니다.

Route 53 ARC에서 준비 확인 생성 및 업데이트

이 섹션에서는 리소스의 생성, 업데이트, 삭제를 포함하여 준비 상태 검사 및 리소스 세트에 대한 절차를 제공합니다.

준비 확인 생성 및 업데이트

이 섹션의 단계에서는 Route 53 ARC 콘솔에서 준비 확인을 생성하는 방법을 설명합니다. Amazon Route 53 Application Recovery Controller에서 복구 준비 API 작업을 사용하는 방법을 보려면 준비 검사 API 작업 섹션을 참조하세요.

준비 확인을 업데이트하려면 준비 확인을 위한 리소스 세트를 편집하거나, 리소스를 추가 또는 제거하거나, 리소스의 준비 범위를 변경할 수 있습니다.

준비 확인 생성

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 준비 확인을 선택합니다.
3. 준비 페이지에서 생성을 선택한 다음 준비 확인을 선택합니다.
4. 준비 확인의 이름을 입력하고 확인하려는 리소스 유형을 선택한 후 다음을 선택합니다.
5. 준비 확인을 위한 리소스 세트를 추가합니다. 리소스 세트는 서로 다른 복제본에 있는 동일한 유형의 리소스 그룹입니다. 다음 중 하나를 선택합니다.

   - 이미 생성한 리소스 세트의 리소스로 준비 확인을 생성합니다.
   - 새 리소스 세트를 생성합니다.

   새 리소스 세트를 생성하도록 선택하는 경우 리소스 세트의 이름을 입력하고 추가를 선택합니다.
6. 세트에 포함시키려는 각 리소스에 대해 Amazon 리소스 이름(ARN)을 하나씩 복사하여 붙여넣은 후 다음을 선택합니다.

   > **Tip**
   >
   > Route 53 ARC가 각 리소스 유형에 대해 예상하는 ARN 형식에 대한 예제 및 자세한 내용은 Route 53 ARC의 리소스 유형 및 ARN 형식 섹션을 참조하세요.
7. 원하는 경우 Route 53 ARC가 이 준비 확인에 포함된 리소스 유형을 확인할 때 사용되는 준비 규칙을 확인합니다. 다음을 선택합니다.
8. (선택 사항) 복구 그룹 이름에서 준비 확인을 연결할 복구 그룹을 선택한 다음 각 리소스 ARN에 대해 리소스가 속한 드롭다운 메뉴에서 셀(리전 또는 가용 영역)을 선택합니다. DNS 라우팅 정책과 같은 애플리케이션 수준 리소스인 경우 글로벌 리소스(셀 없음)를 선택합니다.

   이는 준비 확인의 리소스에 대한 준비 범위를 지정합니다.

   > **Important**
   >
   > 이 단계는 선택 사항이지만 복구 그룹 및 셀에 대한 요약 준비 정보를 가져오려면 준비 범위를 추가해야 합니다. 이 단계를 건너뛰고 여기에서 준비 범위를 선택하여 준비 확인을 복구 그룹의 리소스와 연결하지 않는 경우 Route 53 ARC는 복구 그룹 또는 셀에 대한 요약 준비 정보를 반환할 수 없습니다.

9. 다음을 선택합니다.
10. 확인 페이지의 정보를 검토한 다음 준비 확인 생성을 선택합니다.

준비 확인 삭제

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 준비 확인을 선택합니다.
3. 준비 확인을 선택하고 작업에서 삭제를 선택합니다.

리소스 세트 생성 및 편집

일반적으로 준비 확인 생성의 일부로 리소스 세트를 생성하지만 리소스 세트를 별도로 생성할 수도 있습니다. 리소스 세트를 편집하여 리소스를 추가하거나 제거할 수도 있습니다. 이 섹션의 단계에서는 Route 53 ARC 콘솔에서 준비 확인을 생성하는 방법을 설명합니다. Amazon Route 53 Application Recovery Controller에서 복구 준비 API 작업을 사용하는 방법을 보려면 준비 검사 API 작업 섹션을 참조하세요.

리소스 세트 생성

1. https://console.aws.amazon.com/route53/home에서 Route 53 콘솔을 엽니다.
2. Application Recovery Controller에서 리소스 세트를 선택합니다.
3. 생성을 선택합니다.
4. 리소스 세트의 이름을 입력한 다음 세트에 포함할 리소스 유형을 선택합니다.
5. 추가를 선택한 다음 세트에 추가할 리소스의 Amazon 리소스 이름(ARN)을 입력합니다.
6. 리소스 추가를 완료한 후 리소스 세트 생성을 선택합니다.

리소스 세트 편집

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 준비 확인을 선택합니다.
3. 리소스 세트에서 작업을 선택한 다음 편집을 선택합니다.
4. 다음 중 하나를 수행하십시오.

- 세트에서 리소스를 제거하려면 제거를 선택합니다.
- 세트에 리소스를 추가하려면 추가를 선택한 다음 리소스의 Amazon 리소스 이름(ARN)을 입력합니다.

5. 또한 리소스의 준비 범위를 편집하여 준비 확인을 위해 리소스를 다른 셀과 연결할 수도 있습니다.
6. 저장을 선택합니다.

Route 53 ARC에서의 준비 확인 모니터링

Amazon Route 53 Application Recovery Controller에서 애플리케이션의 준비 확인을 볼 수 있습니다.

- 리소스 세트의 리소스에 대한 준비 확인 수준
- 개별 리소스 수준
- 가용 영역 또는 AWS 지역의 모든 리소스에 대한 셀 (애플리케이션 복제본) 수준
- 애플리케이션 전체의 복구 그룹 수준

준비 확인 변경에 대한 알림을 받거나 Route 53 콘솔에서 또는 Route 53 ARC CLI 명령을 사용하여 준비 상태 변경을 모니터링할 수 있습니다.

준비 상태 알림

EventBridge Amazon을 사용하여 Route 53 ARC 리소스를 모니터링하고 준비 상태 변경을 알리는 이벤트 기반 규칙을 설정할 수 있습니다. 자세한 정보는 Amazon에서 Route 53 ARC에서 준비 상태 확인 사용하기 EventBridge을 참조하세요.

Route 53 ARC 콘솔에서 준비 상태 모니터링

다음 절차는 에서 복구 준비 상태를 모니터링하는 방법을 설명합니다. AWS Management Console

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 준비 확인을 선택합니다.
3. 준비 페이지의 복구 그룹에서 각 복구 그룹(애플리케이션)의 복구 그룹 준비 상태를 확인합니다.

   특정 셀 또는 개별 리소스의 준비도 볼 수 있습니다.

CLI 명령을 사용하여 준비 상태 모니터링

이 섹션에서는 다양한 수준에서 애플리케이션 및 리소스의 준비 상태를 확인하는 데 사용할 수 있는 AWS CLI 명령의 예를 제공합니다.

리소스 세트 준비

리소스 세트(리소스 그룹)에 대해 생성한 준비 확인의 상태입니다.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-
status --readiness-check-name ReadinessCheckName
```

단일 리소스에 대한 준비

각 준비 규칙의 상태를 포함하여 준비 확인에서 단일 리소스의 상태를 가져오려면 준비 확인 이름 및 리소스 ARN을 지정합니다. 예:

```
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"
```

셀 준비

단일 셀, 즉 리전 또는 가용 영역의 상태입니다.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-
summary --cell-name CellName
```

애플리케이션 준비

복구 그룹 수준에서의 전체 애플리케이션 상태입니다.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-
readiness-summary --recovery-group-name RecoveryGroupName
```

Route 53 ARC에서 아키텍처 권장 사항 확인하기

기존 애플리케이션이 있는 경우, Amazon Route 53 Application Recovery Controller는 애플리케이션 및 라우팅 정책의 아키텍처를 평가하여 애플리케이션의 복구 복원력을 향상하도록 설계를 수정하기 위한 권장 사항을 제공할 수 있습니다. Route 53 ARC에서 애플리케이션을 나타내는 복구 그룹을 생성한 후, 이 섹션의 단계에 따라 애플리케이션 아키텍처에 대한 권장 사항을 확인합니다.

복구 그룹의 DNS 대상 리소스를 아직 지정하지 않았다면 보다 자세한 권장 사항을 제공할 수 있도록 대상 리소스를 지정하는 것이 좋습니다. 추가 정보를 제공하면 Route 53 ARC가 더 나은 권장 사항을 제공할 수 있습니다. 예를 들어 Amazon Route 53 리소스 레코드 또는 Network Load Balancer를 대상 리소스로 입력하면 Route 53 ARC는 복구 그룹에 맞는 최적의 셀 수를 생성했는지 여부에 대한 정보를 제공할 수 있습니다.

DNS 대상 리소스의 경우 다음을 참고하세요.

- 대상 리소스에는 Route 53 리소스 레코드 또는 Network Load Balancer만 지정합니다.
- 각 복구 그룹에 대해 DNS 대상 리소스를 하나만 생성합니다.
- 권장: 각 셀에 대해 DNS 대상 리소스를 하나 생성합니다.
- 준비 확인을 통해 DNS 대상 리소스를 하나의 리소스 세트로 그룹화합니다.

다음 절차에서는 DNS 대상 리소스를 생성하는 방법 및 애플리케이션에 대한 아키텍처 권장 사항을 확인하는 방법을 설명합니다.

아키텍처 업데이트에 대한 권장 사항 확인

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 준비 확인을 선택합니다.
3. 복구 그룹 이름에서 애플리케이션을 나타내는 복구 그룹을 선택합니다.
4. 복구 그룹 세부 정보 페이지의 작업 메뉴에서 이 복구 그룹에 대한 아키텍처 권장 사항 확인을 선택합니다.
5. DNS 대상 리소스 준비 확인을 아직 생성하지 않았다면 Route 53 ARC에서 아키텍처 권장 사항을 제공할 수 있도록 새로 생성합니다. DNS 대상 리소스 생성을 선택합니다.

   DNS 대상 리소스에 대한 자세한 내용은 준비 확인 구성 요소 섹션을 참조하세요.
6. DNS 대상 리소스에 대한 리소스 세트를 만들려면 준비 확인을 생성합니다. 준비 확인의 이름을 입력한 다음 준비 확인 유형으로 DNS 대상 리소스를 선택합니다.
7. 리소스 세트 이름을 입력합니다.
8. DNS 이름, 호스팅 영역 ARN, 레코드 세트 ID 등 애플리케이션의 속성을 입력합니다.

> **Tip**
>
> 호스팅 영역 ARN의 형식을 보려면 Route 53 ARC의 리소스 유형 및 ARN 형식에서 호스팅 영역의 ARN 형식을 참조하세요.

선택적 속성 추가를 선택하고 Network Load Balancer ARN 또는 도메인의 Route 53 리소스 레코드를 제공하는 것은 선택 사항이지만 강력하게 권장합니다.

9. (선택 사항) 복구 그룹 구성에서 DNS 대상 리소스의 셀을 선택하여 준비 범위를 설정합니다.
10. 리소스 세트 생성을 선택합니다.
11. 복구 그룹 세부 정보 페이지에서 아키텍처 권장 사항 확인을 선택합니다. Route 53 ARC는 페이지에 일련의 권장 사항을 표시합니다.

권장 사항 목록을 검토합니다. 그런 다음 앱의 복구 복원력을 개선하기 위한 변경 여부와 변경 방법을 결정할 수 있습니다.

Route 53 ARC에서 교차 계정 권한 생성

리소스가 여러 AWS 계정에 분산되어 있어 애플리케이션 상태를 종합적으로 파악하기 어려울 수 있습니다. 또한 빠른 결정을 내리는 데 필요한 정보를 얻기가 어려울 수도 있습니다. Amazon Route 53 애플리케이션 복구 컨트롤러에서 준비 상태 검사를 간소화하기 위해 계정 간 인증을 사용할 수 있습니다.

Route 53 ARC의 크로스 계정 승인은 준비 확인 기능과 함께 작동합니다. 교차 계정 인증을 사용하면 하나의 중앙 AWS 계정을 사용하여 여러 계정에 있는 리소스를 모니터링할 수 있습니다. AWS 모니터링하려는 리소스가 있는 각 계정에서 해당 리소스에 액세스할 수 있도록 중앙 계정을 승인합니다. 그러면 중앙 계정에서 모든 계정의 리소스에 대한 준비 확인을 생성하고 중앙 계정에서 장애 조치 준비를 모니터링할 수 있습니다.

> **Note**
>
> 크로스 계정 권한 부여는 콘솔에서 설정할 수 없습니다. 대신 Route 53 ARC API 작업을 사용하여 크로스 계정 인증을 설정하고 사용합니다. 시작하는 데 도움이 되도록 이 섹션에서는 AWS CLI 명령 예제를 제공합니다.

미국 서부(오레곤) 리전(us-west-2)에 리소스가 있는 계정이 있고 미국 동부(버지니아 북부) 리전(us-east-1)에서 모니터링하려는 리소스가 있는 계정도 있다고 가정해 보겠습니다. Route 53 ARC를 사용

하면 크로스 계정 인증을 사용하여 us-west-2 계정 하나에서 두 리소스 세트를 모두 모니터링할 수 있습니다.

예를 들어 다음과 같은 AWS 계정이 있다고 가정해 보겠습니다.

- 미국 서부 계정: 999999999999
- 미국 동부 계정: 111111111111

us-east-1 계정(111111111111)에서 us-west-2 IAM 계정 `arn:aws:iam::999999999999:root`의 (루트) 사용자에 대한 Amazon 리소스 이름(ARN)을 지정하여 us-west-2 계정(999999999999)의 액세스를 허용하도록 크로스 계정 인증을 활성화할 수 있습니다. 권한을 생성한 후 us-west-2 계정은 us-east-1이 소유한 리소스를 리소스 세트에 추가하고 리소스 세트에서 실행할 준비 확인을 생성할 수 있습니다.

다음 예는 한 계정에 대한 크로스 계정 권한 부여를 설정하는 방법을 보여줍니다. Route 53 ARC에서 추가하고 모니터링하려는 AWS 리소스가 있는 각 추가 계정에서 교차 계정 인증을 활성화해야 합니다.

> **Note**
>
> Route 53 ARC는 여러 AWS 지역의 엔드포인트를 지원하는 글로벌 서비스이지만 대부분의 Route 53 ARC CLI 명령에서 미국 서부 (오레곤) 지역을 지정 (즉, 파라미터 지정`--region us-west-2`) 해야 합니다.

다음 AWS CLI 명령은 이 예제에서 교차 계정 인증을 설정하는 방법을 보여줍니다.

```
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
```

이 권한을 사용하지 않도록 설정하려면 다음을 수행합니다.

```
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
```

크로스 계정 승인을 제공한 모든 계정의 특정 계정을 확인하려면 `list-cross-account-authorizations` 명령을 사용합니다. 이때 다른 방향으로는 확인할 수 없습니다. 즉, 계정 프로필과 함께 리소스를 추가하고 모니터링할 수 있는 크로스 계정 권한이 부여된 모든 계정을 나열하는 데 사용할 수 있는 API 작업은 없습니다.

```
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"
    ]
}
```

준비 규칙, 리소스 유형 및 ARNS

이 섹션에는 준비 상태 규칙 설명, 지원되는 리소스 유형 및 리소스 세트에 사용하는 Amazon Resource Names (ARN) 형식에 대한 참조 정보가 포함되어 있습니다.

Route 53 ARC의 준비 규칙 설명

이 섹션에는 Amazon Route 53 Application Recovery Controller가 지원하는 모든 유형의 리소스에 대한 준비 규칙 설명이 나열되어 있습니다. Route 53 ARC에서 지원하는 리소스 유형의 목록을 보려면 Route 53 ARC의 리소스 유형 및 ARN 형식 섹션을 참조하세요.

Route 53 ARC 콘솔에서 또는 API 작업을 통해 다음을 수행하여 준비 규칙 설명을 볼 수도 있습니다.

- 콘솔에서 준비 규칙을 보려면 다음 절차의 단계를 따릅니다. 콘솔에서 준비 규칙 보기
- API를 사용하여 준비 규칙을 보려면 작업을 참조하십시오. ListRules

주제

- Route 53 ARC의 준비 규칙
- 콘솔에서 준비 규칙 보기

Route 53 ARC의 준비 규칙

이 섹션에는 Route 53 ARC에서 지원하는 각 리소스 유형에 대한 준비 규칙 세트가 나열되어 있습니다.

규칙 설명을 살펴보면 대부분의 규칙 설명에 모두 검사 또는 각각 검사라는 용어가 포함되어 있음을 알 수 있습니다. 이러한 용어가 준비 확인의 맥락에서 규칙이 작동하는 방식을 설명하는 방법과 Route 53 ARC가 준비 상태를 설정하는 방법에 대한 기타 세부 정보를 이해하려면 준비 규칙이 준비 상태를 결정하는 방법을 참조하세요.

준비 규칙

Route 53 ARC는 다음과 같은 준비 규칙을 사용하여 리소스를 감사합니다.

Amazon API Gateway 버전 1단계

- ApiGwV1ApiKeyCount: 모든 API Gateway 단계를 검사하여 동일한 수의 API 키가 연결되어 있는지 확인합니다.
- ApiGwV1ApiKeySource: 모든 API Gateway 단계를 검사하여 `API Key Source` 값이 동일한지 확인합니다.
- ApiGwV1BasePath: 모든 API Gateway 단계를 검사하여 동일한 기반 경로에 연결되어 있는지 확인합니다.
- ApiGwV1BinaryMediaTypes: 모든 API Gateway 단계를 검사하여 동일한 바이너리 미디어 유형을 지원하는지 확인합니다.
- ApiGwV1CacheClusterEnabled: 모든 API Gateway 단계를 검사하여 `Cache Cluster`가 모두 활성화되었거나 활성화되지 않았는지 확인합니다.
- ApiGwV1CacheClusterSize: 모든 API Gateway 단계를 검사하여 `Cache Cluster Size`가 동일한지 확인합니다. 하나의 값이 더 크면 나머지 값은 NOT READY로 표시됩니다.
- ApiGwV1CacheClusterStatus: 모든 API Gateway 단계를 검사하여 `Cache Cluster`가 AVAILABLE 상태인지 확인합니다.
- ApiGwV1DisableExecuteApiEndpoint: 모든 API Gateway 단계를 검사하여 `Execute API Endpoint`가 모두 비활성화되었거나 비활성화되지 않았는지 확인합니다.
- ApiGwV1DomainName: 모든 API Gateway 단계를 검사하여 동일한 도메인 이름에 연결되어 있는지 확인합니다.
- ApiGwV1EndpointConfiguration: 모든 API Gateway 단계를 검사하여 동일한 엔드포인트 구성의 도메인에 연결되어 있는지 확인합니다.

- ApiGwV1EndpointDomainNameStatus: 모든 API Gateway 단계를 검사하여 연결된 도메인 이름이 AVAILABLE 상태인지 확인합니다.
- ApiGwV1MethodSettings: 모든 API Gateway 단계를 검사하여 `Method Settings` 값이 동일한지 확인합니다.
- ApiGwV1MutualTlsAuthentication: 모든 API Gateway 단계를 검사하여 `Mutual TLS Authentication` 값이 동일한지 확인합니다.
- ApiGwV1Policy: 모든 API Gateway 단계를 검사하여 모두 API 수준 정책을 사용하거나 사용하지 않는지 확인합니다.
- ApiGwV1RegionalDomainName: 모든 API Gateway 단계를 검사하여 동일한 리전별 도메인 이름에 연결되어 있는지 확인합니다. 참고: 이 규칙은 준비 상태에는 영향을 미치지 않습니다.
- ApiGwV1ResourceMethodConfigs: 모든 API Gateway 단계를 검사하여 관련 구성을 포함하여 리소스 계층 구조가 유사한지 확인합니다.
- ApiGwV1SecurityPolicy: 모든 API Gateway 단계를 검사하여 `Security Policy` 값이 동일한지 확인합니다.
- ApiGwV1Quotas: 모든 API Gateway 그룹을 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.
- ApiGwV1UsagePlans: 모든 API Gateway 단계를 검사하여 동일한 구성의 `Usage Plans`에 연결되어 있는지 확인합니다.

Amazon API Gateway 버전 2단계

- ApiGwV2ApiKeySelectionExpression: 모든 API Gateway 단계를 검사하여 `API Key Selection Expression` 값이 동일한지 확인합니다.
- ApiGwV2ApiMappingSelectionExpression: 모든 API Gateway 단계를 검사하여 `API Mapping Selection Expression` 값이 동일한지 확인합니다.
- ApiGwV2CorsConfiguration: 모든 API Gateway 단계를 검사하여 CORS 관련 구성이 동일한지 확인합니다.
- ApiGwV2DomainName: 모든 API Gateway 단계를 검사하여 동일한 도메인 이름에 연결되어 있는지 확인합니다.
- ApiGwV2DomainNameStatus: 모든 API Gateway 단계를 검사하여 도메인 이름이 AVAILABLE 상태인지 확인합니다.
- ApiGwV2EndpointType: 모든 API Gateway 단계를 검사하여 `Endpoint Type` 값이 동일한지 확인합니다.
- ApiGwV2Quotas: 모든 API Gateway 그룹을 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

- ApiGwV2MutualTlsAuthentication: 모든 API Gateway 단계를 검사하여 `Mutual TLS Authentication` 값이 동일한지 확인합니다.
- ApiGwV2ProtocolType: 모든 API Gateway 단계를 검사하여 `Protocol Type` 값이 동일한지 확인합니다.
- ApiGwV2RouteConfigs: 모든 API Gateway 단계를 검사하여 동일한 구성의 경로 계층 구조가 동일한지 확인합니다.
- ApiGwV2RouteSelectionExpression: 모든 API Gateway 단계를 검사하여 `Route Selection Expression` 값이 동일한지 확인합니다.
- ApiGwV2RouteSettings: 모든 API Gateway 단계를 검사하여 `Default Route Settings` 값이 동일한지 확인합니다.
- ApiGwV2SecurityPolicy: 모든 API Gateway 단계를 검사하여 `Security Policy` 값이 동일한지 확인합니다.
- ApiGwV2StageVariables: 모든 API Gateway 단계를 검사하여 모든 `Stage Variables`가 다른 단계와 동일한지 확인합니다.
- ApiGwV2ThrottlingBurstLimit: 모든 API Gateway 단계를 검사하여 `Throttling Burst Limit` 값이 동일한지 확인합니다.
- ApiGwV2ThrottlingRateLimit: 모든 API Gateway 단계를 검사하여 `Throttling Rate Limit` 값이 동일한지 확인합니다.

Amazon Aurora 클러스터

- RdsClusterStatus: 각 Aurora 클러스터를 검사하여 상태가 `AVAILABLE` 또는 `BACKING-UP`인지 확인합니다.
- RdsEngineMode: 모든 Aurora 클러스터를 검사하여 `Engine Mode` 값이 동일한지 확인합니다.
- RdsEngineVersion: 모든 Aurora 클러스터를 검사하여 `Major Version` 값이 동일한지 확인합니다.
- RdsGlobalReplicaLag: 각 Aurora 클러스터를 검사하여 `Global Replica Lag` 대기 시간이 30초 미만인지 확인합니다.
- RdsNormalizedCapacity: 모든 Aurora 클러스터를 검사하여 정규화된 용량이 리소스 세트 최대값의 15% 이내인지 확인합니다.
- RdsInstanceType: 모든 Aurora 클러스터를 검사하여 인스턴스 유형이 동일한지 확인합니다.
- RdsQuotas: 모든 Aurora 클러스터를 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

Auto Scaling 그룹

- AsgMinSizeAndMaxSize: 모든 오토 스케일링을 검사하여 최소 및 최대 그룹 크기가 동일한지 확인합니다.
- AsgAZCount: 모든 오토 스케일링을 검사하여 가용 영역 수가 동일한지 확인합니다.
- AsgInstanceTypes: 모든 오토 스케일링을 검사하여 인스턴스 유형이 동일한지 확인합니다. 참고: 이 규칙은 준비 상태에는 영향을 미치지 않습니다.
- AsgInstanceSizes: 모든 오토 스케일링을 검사하여 인스턴스 크기가 동일한지 확인합니다.
- AsgNormalizedCapacity: 모든 오토 스케일링을 검사하여 정규화된 용량이 리소스 세트 최대값의 15% 이내인지 확인합니다.
- AsgQuotas: 모든 오토 스케일링을 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

CloudWatch 알람

- CloudWatchAlarmState: CloudWatch 경보를 검사하여 각 경보가 or 상태가 아닌지 확인합니다. `ALARM` `INSUFFICIENT_DATA`

고객 게이트웨이

- CustomerGatewayIpAddress: 모든 고객 게이트웨이를 검사하여 IP 주소가 동일한지 확인합니다.
- CustomerGatewayState: 고객 게이트웨이를 검사하여 각 게이트웨이가 `AVAILABLE` 상태에 있는지 확인합니다.
- CustomerGatewayVPNType: 모든 고객 게이트웨이를 검사하여 VPN 유형이 동일한지 확인합니다.

DNS target resources

- DnsTargetResourceHostedZoneConfigurationRule: 모든 DNS 대상 리소스를 검사하여 Amazon Route 53 호스팅 영역 ID가 동일한지 및 각 호스팅 영역이 비공개가 아닌지 확인합니다. 참고: 이 규칙은 준비 상태에는 영향을 미치지 않습니다.
- DnsTargetResourceRecordSetConfigurationRule: 모든 DNS 대상 리소스를 검사하여 리소스 레코드 캐시 TTL(Time to Live)이 동일하고 TTL이 300 이하인지 확인합니다.
- DnsTargetResourceRoutingRule: 별칭 리소스 레코드 세트와 연결된 각 DNS 대상 리소스를 검사하여 대상 리소스에 구성된 DNS 이름으로 트래픽을 라우팅하는지 확인합니다. 참고: 이 규칙은 준비 상태에는 영향을 미치지 않습니다.
- DnsTargetResourceHealthCheckRule: 모든 DNS 대상 리소스를 검사하여 적절한 경우 상태 확인이 리소스 레코드 세트와 연결되고 다른 경우에는 연결되지 않는지 확인합니다. 참고: 이 규칙은 준비 상태에는 영향을 미치지 않습니다.

Amazon DynamoDB 테이블

- DynamoConfiguration: 모든 DynamoDB 테이블을 검사하여 키, 속성, 서버 측 암호화 및 스트림 구성이 동일한지 확인합니다.
- DynamoTableStatus: 각 DynamoDB 테이블을 검사하여 상태가 ACTIVE인지 확인합니다.
- DynamoCapacity: 모든 DynamoDB 테이블을 검사하여 프로비저닝된 읽기 용량과 쓰기 용량이 리소스 세트 최대 용량의 20% 이내인지 확인합니다.
- DynamoPeakRcuWcu: 각 DynamoDB 테이블을 검사하여 프로비저닝된 용량을 보장하기 위해 피크 트래픽이 다른 테이블과 유사한지 확인합니다.
- DynamoGsiPeakRcuWcu: 각 DynamoDB 테이블을 검사하여 프로비저닝된 용량을 보장하기 위해 최대 읽기 및 쓰기 용량이 다른 테이블과 유사한지 확인합니다.
- DynamoGsiConfig: 글로벌 보조 인덱스가 있는 모든 DynamoDB 테이블을 검사하여 테이블이 동일한 인덱스, 키 스키마 및 프로젝션을 사용하는지 확인합니다.
- DynamoGsiStatus: 글로벌 보조 인덱스가 있는 모든 DynamoDB 테이블을 검사하여 글로벌 보조 인덱스가 ACTIVE 상태인지 확인합니다.
- DynamoGsiCapacity: 글로벌 보조 인덱스가 있는 모든 DynamoDB 테이블을 검사하여 프로비저닝된 GSI 읽기 용량과 GSI 쓰기 용량이 리소스 세트 최대 용량의 20% 이내인지 확인합니다.
- DynamoReplicationLatency: 글로벌 테이블인 모든 DynamoDB 테이블을 검사하여 복제 지연 시간이 동일한지 확인합니다.
- DynamoAutoScalingConfiguration: Auto Scaling이 활성화된 모든 DynamoDB 테이블을 검사하여 최소, 최대, 대상 읽기 및 쓰기 용량이 동일한지 확인합니다.
- DynamoQuotas: 모든 DynamoDB 테이블을 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

Elastic Load Balancing(Classic Load Balancer)

- ElbV1CheckAzCount: 각 Classic Load Balancer를 검사하여 하나의 가용 영역에만 연결되어 있는지 확인합니다. 참고: 이 규칙은 준비 상태에는 영향을 미치지 않습니다.
- ElbV1AnyInstances: 모든 Classic Load Balancer를 검사하여 하나 이상의 EC2 인스턴스가 있는지 확인합니다.
- ElbV1AnyInstancesHealthy: 모든 Classic Load Balancer를 검사하여 하나 이상의 정상적인 EC2 인스턴스가 있는지 확인합니다.
- ElbV1Scheme: 모든 Classic Load Balancer를 검사하여 로드 밸런서 체계가 동일한지 확인합니다.
- ElbV1HealthCheckThreshold: 모든 Classic Load Balancer를 검사하여 상태 확인 임계값이 동일한지 확인합니다.

- ElbV1HealthCheckInterval: 모든 Classic Load Balancer를 검사하여 상태 확인 간격 값이 동일한지 확인합니다.
- ElbV1CrossZoneRoutingEnabled: 모든 Classic Load Balancer를 검사하여 영역 간 로드 밸런서 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV1AccessLogsEnabledAttribute: 모든 Classic Load Balancer를 검사하여 액세스 로그 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV1ConnectionDrainingEnabledAttribute: 모든 Classic Load Balancer를 검사하여 Connection Draining 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV1ConnectionDrainingTimeoutAttribute: 모든 Classic Load Balancer를 검사하여 Connection Draining 제한 시간 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV1IdleTimeoutAttribute: 모든 Classic Load Balancer를 검사하여 유휴 제한 시간 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV1ProvisionedCapacityLcuCount: 프로비저닝된 LCU가 10개 이상인 모든 Classic Load Balancer를 검사하여 리소스 세트에서 프로비저닝된 LCU가 가장 높은 LCU의 20% 이내인지 확인합니다.
- ElbV1ProvisionedCapacityStatus: 각 Classic Load Balancer의 프로비저닝된 용량 상태를 검사하여 DISABLED 또는 PENDING 값이 아닌지 확인합니다.

Amazon EBS 볼륨

- EbsVolumeEncryption: 모든 EBS 볼륨을 검사하여 암호화 값(ENABLED 또는 DISABLED)이 동일한지 확인합니다.
- EbsVolumeEncryptionDefault: 모든 EBS 볼륨을 검사하여 기본적으로 암호화 값(ENABLED 또는 DISABLED)이 동일한지 확인합니다.
- EbsVolumeIops: 모든 EBS 볼륨을 검사하여 초당 입출력 작업 처리량(IOPS)이 동일한지 확인합니다.
- EbsVolumeKmsKeyId: 모든 EBS 볼륨을 검사하여 기본 AWS KMS 키 ID가 동일한지 확인합니다.
- EbsVolumeMultiAttach: 모든 EBS 볼륨을 검사하여 다중 연결 값(ENABLED 또는 DISABLED)이 동일한지 확인합니다.
- EbsVolumeQuotas: 모든 EBS 볼륨을 검사하여 Service Quotas에서 설정한 할당량(제한)을 준수하는지 확인합니다.
- EbsVolumeSize: 모든 EBS 볼륨을 검사하여 읽기 가능한 크기가 동일한지 확인합니다.
- EbsVolumeState: 모든 EBS 볼륨을 검사하여 볼륨 상태가 동일한지 확인합니다.
- EbsVolumeType: 모든 EBS 볼륨을 검사하여 볼륨 유형이 동일한지 확인합니다.

AWS Lambda 함수

- LambdaMemorySize: 모든 Lambda 함수를 검사하여 메모리 크기가 동일한지 확인합니다. 하나의 메모리가 더 많으면 나머지 메모리는 `NOT READY`로 표시됩니다.
- LambdaFunctionTimeout: 모든 Lambda 함수를 검사하여 제한 시간 값이 동일한지 확인합니다. 하나의 값이 더 크면 나머지 값은 `NOT READY`로 표시됩니다.
- LambdaFunctionRuntime: 모든 Lambda 함수를 검사하여 모두 런타임이 동일한지 확인합니다.
- LambdaFunctionReservedConcurrentExecutions: 모든 Lambda 함수를 검사하여 모두 `Reserved Concurrent Executions` 값이 동일한지 확인합니다. 하나의 값이 더 크면 나머지 값은 `NOT READY`로 표시됩니다.
- LambdaFunctionDeadLetterConfig: 모든 Lambda 함수를 검사하여 모두 `Dead Letter Config`가 정의되어 있거나 정의되어 있지 않은지 확인합니다.
- LambdaFunctionProvisionedConcurrencyConfig: 모든 Lambda 함수를 검사하여 `Provisioned Concurrency` 값이 동일한지 확인합니다.
- LambdaFunctionSecurityGroupCount: 모든 Lambda 함수를 검사하여 `Security Groups` 값이 동일한지 확인합니다.
- LambdaFunctionSubnetIdCount: 모든 Lambda 함수를 검사하여 `Subnet Ids` 값이 동일한지 확인합니다.
- LambdaFunctionEventSourceMappingMatch: 모든 Lambda 함수를 검사하여 선택한 모든 `Event Source Mapping` 속성이 함수 간에 일치하는지 확인합니다.
- LambdaFunctionLimitsRule: 모든 Lambda 함수를 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

Network Load Balancer 및 Application Load Balancer

- ElbV2CheckAzCount: 각 Network Load Balancer를 검사하여 하나의 가용 영역에만 연결되어 있는지 확인합니다. 참고: 이 규칙은 준비 상태에는 영향을 미치지 않습니다.
- ElbV2TargetGroupsCanServeTraffic: 각 Network Load Balancer 및 Application Load Balancer를 검사하여 정상적인 Amazon EC2 인스턴스가 하나 이상 있는지 확인합니다.
- ElbV2State: 각 Network Load Balancer 및 Application Load Balancer를 검사하여 `ACTIVE`상태에 있는지 확인합니다.
- ElbV2IpAddressType: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 IP 주소 유형이 동일한지 확인합니다.
- ElbV2Scheme: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 체계가 동일한지 확인합니다.

- ElbV2Type: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 유형이 동일한지 확인합니다.
- ElbV2S3LogsEnabled: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 Amazon S3 서버 액세스 로그 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV2DeletionProtection: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 삭제 보호 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV2IdleTimeoutSeconds: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 유휴 제한 시간 값이 동일한지 확인합니다.
- ElbV2HttpDropInvalidHeaders: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 HTTP 드롭 잘못된 헤더 값이 동일한지 확인합니다.
- ElbV2Http2Enabled: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 HTTP2 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV2CrossZoneEnabled: 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 영역 간 로드 밸런서 값이 동일한지(ENABLED 또는 DISABLED) 확인합니다.
- ElbV2ProvisionedCapacityLcuCount: 프로비저닝된 LCU가 10개 이상인 모든 Network Load Balancer 및 Application Load Balancer를 검사하여 리소스 세트에서 프로비저닝된 LCU가 가장 높은 LCU의 20% 이내인지 확인합니다.
- ElbV2ProvisionedCapacityEnabled: 모든 Network Load Balancer 및 Application Load Balancer의 프로비저닝된 용량 상태를 검사하여 DISABLED 또는 PENDING 값이 아닌지 확인합니다.

Amazon MSK 클러스터

- MskClusterClientSubnet: 각 MSK 클러스터를 검사하여 클라이언트 서브넷이 2개 또는 3개만 있는지 확인합니다.
- MskClusterInstanceType: 모든 MSK 클러스터를 검사하여 Amazon EC2 인스턴스 유형이 동일한지 확인합니다.
- MskClusterSecurityGroups: 모든 MSK 클러스터를 검사하여 보안 그룹이 동일한지 확인합니다.
- MskClusterStorageInfo: 모든 MSK 클러스터를 검사하여 EBS 스토리지 볼륨 크기가 동일한지 확인합니다. 하나의 값이 더 크면 나머지 값은 NOT READY로 표시됩니다.
- MskClusterACMCertificate: 모든 MSK 클러스터를 검사하여 클라이언트 권한 부여 인증서 ARN 목록이 동일한지 확인합니다.
- MskClusterServerProperties: 모든 MSK 클러스터를 검사하여 `Current Broker Software Info` 값이 동일한지 확인합니다.
- MskClusterKafkaVersion: 모든 MSK 클러스터를 검사하여 Kafka 버전이 동일한지 확인합니다.

- MskClusterEncryptionInTransitInCluster: 모든 MSK 클러스터를 검사하여 `Encryption In Transit In Cluster` 값이 동일한지 확인합니다.
- MskClusterEncryptionInClientBroker: 모든 MSK 클러스터를 검사하여 `Encryption In Transit Client Broker` 값이 동일한지 확인합니다.
- MskClusterEnhancedMonitoring: 모든 MSK 클러스터를 검사하여 `Enhanced Monitoring` 값이 동일한지 확인합니다.
- MskClusterOpenMonitoringInJmx: 모든 MSK 클러스터를 검사하여 `Open Monitoring JMX Exporter` 값이 동일한지 확인합니다.
- MskClusterOpenMonitoringInNode: 모든 MSK 클러스터를 검사하여 `Open Monitoring Not Exporter.` 값이 동일한지 확인합니다.
- MskClusterLoggingInS3: 모든 MSK 클러스터를 검사하여 `Is Logging in S3` 값이 동일한지 확인합니다.
- MskClusterLoggingInFirehose: 모든 MSK 클러스터를 검사하여 `Is Logging In Firehose` 값이 동일한지 확인합니다.
- MskClusterLoggingInCloudWatch: 모든 MSK 클러스터를 검사하여 `Is Logging Available In CloudWatch Logs` 값이 동일한지 확인합니다.
- MskClusterNumberOfBrokerNodes: 모든 MSK 클러스터를 검사하여 `Number of Broker Nodes` 값이 동일한지 확인합니다. 하나의 값이 더 크면 나머지 값은 NOT READY로 표시됩니다.
- MskClusterState: 각 MSK 클러스터를 검사하여 ACTIVE 상태인지 확인합니다.
- MskClusterLimitsRule: 모든 Lambda 함수를 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

Amazon Route 53 상태 확인

- R53HealthCheckType: 각 Route 53 상태 확인을 검사하여 CALCULATED 유형이 아닌지 및 모든 검사가 동일한 유형인지 확인합니다.
- R53HealthCheckDisabled: 각 Route 53 상태 확인을 검사하여 DISABLED 상태가 아닌지 확인합니다.
- R53HealthCheckStatus: 각 Route 53 상태 확인을 검사하여 SUCCESS 상태인지 확인합니다.
- R53HealthCheckRequestInterval: 모든 Route 53 상태 확인을 검사하여 모두 `Request Interval` 값이 동일한지 확인합니다.
- R53HealthCheckFailureThreshold: 모든 Route 53 상태 확인을 검사하여 모두 `Failure Threshold.` 값이 동일한지 확인합니다.
- R53HealthCheckEnableSNI: 모든 Route 53 상태 확인을 검사하여 모두 `Enable SNI.` 값이 동일한지 확인합니다.

- R53HealthCheckSearchString: 모든 Route 53 상태 확인을 검사하여 모두 `Search String.` 값이 동일한지 확인합니다.
- R53HealthCheckRegions: 모든 Route 53 상태 확인을 검사하여 모두 AWS 리전 목록이 동일한지 확인합니다.
- R53HealthCheckMeasureLatency: 모든 Route 53 상태 확인을 검사하여 모두 `Measure Latency` 값이 동일한지 확인합니다.
- R53HealthCheckInsufficientDataHealthStatus: 모든 Route 53 상태 확인을 검사하여 모두 `Insufficient Data Health Status` 값이 동일한지 확인합니다.
- R53HealthCheckInverted: 모든 Route 53 상태 확인을 검사하여 모두 반전되었거나 반전되지 않았는지 확인합니다.
- R53HealthCheckResourcePath: 모든 Route 53 상태 확인을 검사하여 모두 `Resource Path` 값이 동일한지 확인합니다.
- R53HealthCheckCloudWatchAlarm: 모든 Route 53 상태 점검을 검사하여 관련 CloudWatch 경보의 설정 및 구성이 동일한지 확인합니다.

Amazon SNS 구독

- SnsSubscriptionProtocol: 모든 SNS 구독을 검사하여 프로토콜이 동일한지 확인합니다.
- SnsSubscriptionSqsLambdaEndpoint: Lambda 또는 SQS 엔드포인트가 있는 모든 SNS 구독을 검사하여 엔드포인트가 서로 다른지 확인합니다.
- SnsSubscriptionNonAwsEndpoint: 비AWS 서비스 엔드포인트 유형 (예: 이메일) 을 가진 모든 SNS 구독을 검사하여 구독의 엔드포인트가 동일한지 확인합니다.
- SnsSubscriptionPendingConfirmation: 모든 SNS 구독을 검사하여 '확인 보류 중' 값이 동일한지 확인합니다.
- SnsSubscriptionDeliveryPolicy: HTTP/S를 사용하는 모든 SNS 구독을 검사하여 '유효 전송 기간' 값이 동일한지 확인합니다.
- SnsSubscriptionRawMessageDelivery: HTTP/S를 사용하는 모든 SNS 구독을 검사하여 '원시 메시지 전송' 값이 동일한지 확인합니다.
- SnsSubscriptionFilter: 모든 SNS 구독을 검사하여 '필터 정책' 값이 동일한지 확인합니다.
- SnsSubscriptionRedrivePolicy: 모든 SNS 구독을 검사하여 '필터 정책' 값이 동일한지 확인합니다.
- SnsSubscriptionEndpointEnabled: 모든 SNS 구독을 검사하여 '엔드포인트 활성화' 값이 동일한지 확인합니다.
- SnsSubscriptionLambdaEndpointValid: Lambda 엔드포인트가 있는 모든 SNS 구독을 검사하여 Lambda 엔드포인트가 유효한지 확인합니다.

- SnsSubscriptionSqsEndpointValidRule: SQS 엔드포인트가 있는 모든 SNS 구독을 검사하여 SQS 엔드포인트가 유효한지 확인합니다.
- SnsSubscriptionQuotas: 모든 SNS 구독을 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

Amazon SNS 주제

- SnsTopicDisplayName: 모든 SNS 주제를 검사하여 `Display Name` 값이 동일한지 확인합니다.
- SnsTopicDeliveryPolicy: HTTPS 구독자가 있는 모든 SNS 주제를 검사하여 `EffectiveDeliveryPolicy`가 동일한지 확인합니다.
- SnsTopicSubscription: 모든 SNS 주제를 검사하여 각 프로토콜의 구독자 수가 동일한지 확인합니다.
- SnsTopicAwsKmsKey: 모든 SNS 주제를 검사하여 모든 주제에 하나의 AWS KMS 키가 있는거나 하나도 없는지 확인합니다.
- SnsTopicQuotas: 모든 SNS 주제를 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

Amazon SQS 대기열

- SqsQueueType: 모든 SQS 대기열을 검사하여 모두 `Type` 값이 동일한지 확인합니다.
- SqsQueueDelaySeconds: 모든 SQS 대기열을 검사하여 모두 `Delay Seconds` 값이 동일한지 확인합니다.
- SqsQueueMaximumMessageSize: 모든 SQS 대기열을 검사하여 모두 `Maximum Message Size` 값이 동일한지 확인합니다.
- SqsQueueMessageRetentionPeriod: 모든 SQS 대기열을 검사하여 모두 `Message Retention Period` 값이 동일한지 확인합니다.
- SqsQueueReceiveMessageWaitTimeSeconds: 모든 SQS 대기열을 검사하여 모두 `Receive Message Wait Time Seconds` 값이 동일한지 확인합니다.
- SqsQueueRedrivePolicyMaxReceiveCount: 모든 SQS 대기열을 검사하여 모두 `Redrive Policy Max Receive Count` 값이 동일한지 확인합니다.
- SqsQueueVisibilityTimeout: 모든 SQS 대기열을 검사하여 모두 `Visibility Timeout` 값이 동일한지 확인합니다.
- SqsQueueContentBasedDeduplication: 모든 SQS 대기열을 검사하여 모두 `Content-Based Deduplication` 값이 동일한지 확인합니다.
- SqsQueueQuotas: 모든 SQS 대기열을 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

Amazon VPC

- VpcCidrBlock: 모든 VPC를 검사하여 모두 CIDR 블록 네트워크 크기 값이 동일한지 확인합니다.
- VpcCidrBlocksSameProtocolVersion: 동일한 CIDR 블록을 가진 모든 VPC를 검사하여 인터넷 스트림 프로토콜 버전 번호의 값이 동일한지 확인합니다.
- VpcCidrBlocksStateInAssociationSets: 모든 VPC의 모든 CIDR 블록 연결 세트를 검사하여 모든 CIDR 블록이 `ASSOCIATED` 상태인지 확인합니다.
- VpcIpv6CidrBlocksStateInAssociationSets: 모든 VPC의 모든 CIDR 블록 연결 세트를 검사하여 모든 CIDR 블록의 주소 수가 동일한지 확인합니다.
- VpcCidrBlocksInAssociationSets: 모든 VPC의 모든 CIDR 블록 연결 세트를 검사하여 모두 크기가 동일한지 확인합니다.
- VpcIpv6CidrBlocksInAssociationSets: 모든 VPC의 모든 IPv6 CIDR 블록 연결 세트를 검사하여 크기가 동일한지 확인합니다.
- VpcState: 각 VPC를 검사하여 `AVAILABLE` 상태인지 확인합니다.
- VpcInstanceTenancy: 모든 VPC를 검사하여 모두 `Instance Tenancy` 값이 동일한지 확인합니다.
- VpcIsDefault: 모든 VPC를 검사하여 `Is Default.` 값이 동일한지 확인합니다.
- VpcSubnetState: 각 VPC 서브넷을 검사하여 AVAILABLE 상태인지 확인합니다.
- VpcSubnetAvailableIpAddressCount: 각 VPC 서브넷을 검사하여 사용 가능한 IP 주소 수가 0보다 큰지 확인합니다.
- VpcSubnetCount: 모든 VPC 서브넷을 검사하여 서브넷 수가 동일한지 확인합니다.
- VpcQuotas: 모든 VPC 서브넷을 검사하여 Service Quotas에서 관리하는 할당량(제한)을 준수하는지 확인합니다.

AWS VPN 연결

- VpnConnectionsRouteCount: 모든 VPN 연결을 검사하여 경로가 하나 이상 있고 경로 수도 동일한지 확인합니다.
- VpnConnectionsEnableAcceleration: 모든 VPC 연결을 검사하여 `Enable Accelerations` 값이 동일한지 확인합니다.
- VpnConnectionsStaticRoutesOnly: 모든 VPC 연결을 검사하여 `Static Routes Only.` 값이 동일한지 확인합니다.
- VpnConnectionsCategory: 모든 VPC 연결을 검사하여 `VPN` 범주가 있는지 확인합니다.
- VpnConnectionsCustomerConfiguration: 모든 VPC 연결을 검사하여 `Customer Gateway Configuration` 값이 동일한지 확인합니다.

- VpnConnectionsCustomerGatewayId: 각 VPN 연결을 검사하여 고객 게이트웨이가 연결되어 있는지 확인합니다.
- VpnConnectionsRoutesState: 모든 VPN 연결을 검사하여 AVAILABLE 상태인지 확인합니다.
- VpnConnectionsVgwTelemetryStatus: 각 VPN 연결을 검사하여 UP의 VGW 상태인지 확인합니다.
- VpnConnectionsVgwTelemetryIpAddress: 각 VPN 연결을 검사하여 각 VGW 원격 분석마다 외부 IP 주소가 다른지 확인합니다.
- VpnConnectionsTunnelOptions: 모든 VPC 연결을 검사하여 터널 옵션이 동일한지 확인합니다.
- VpnConnectionsRoutesCidr: 모든 VPC 연결을 검사하여 대상 CIDR 블록이 동일한지 확인합니다.
- VpnConnectionsInstanceType: 모든 VPC 연결을 검사하여 Instance Type가 동일한지 확인합니다.

AWS VPN 게이트웨이

- VpnGatewayState: 모든 VPN 게이트웨이를 검사하여 AVAILABLE 상태인지 확인합니다.
- VpnGatewayAsn: 모든 VPN 게이트웨이를 검사하여 ASN이 동일한지 확인합니다.
- VpnGatewayType: 모든 VPN 게이트웨이를 검사하여 유형이 동일한지 확인합니다.
- VpnGatewayAttachment: 모든 VPC 게이트웨이를 검사하여 첨부 파일 구성이 동일한지 확인합니다.

콘솔에서 준비 규칙 보기

에서 각 리소스 유형별로 나열된 준비 규칙을 볼 수 있습니다. AWS Management Console

콘솔에서 준비 규칙 보기

1. 에서 Route 53 ARC 콘솔을 엽니다https://console.aws.amazon.com/route53recovery/home#/dashboard.
2. 준비 확인을 선택합니다.
3. 리소스 유형에서 규칙을 보려는 리소스 유형을 선택합니다.

Route 53 ARC의 리소스 유형 및 ARN 형식

Amazon Route 53 Application Recovery Controller에서 리소스 세트를 생성할 때는 세트에 포함할 리소스 유형과 포함할 각 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. Route 53 ARC에서는 각

리소스 유형에 대해 특정 ARN 형식을 예상합니다. 이 섹션에는 Route 53 ARC에서 지원하는 리소스 유형과 각 유형에 대한 관련 ARN 형식이 나열되어 있습니다.

구체적인 형식은 리소스에 따라 다릅니다. ARN을 제공할 때 `####` 텍스트를 리소스별 정보로 바꿉니다.

> **Note**
>
> Route 53 ARC가 리소스에 요구하는 ARN 형식은 서비스 자체가 리소스에 요구하는 ARN 형식과 다를 수 있다는 점에 유의하세요. 예를 들어, 서비스 권한 부여 참조의 각 서비스에 대한 리소스 유형 섹션에 설명된 ARN 형식에는 Route 53 ARC가 Route 53 ARC 서비스의 기능을 지원하는 데 필요한 AWS 계정 ID 또는 기타 정보가 포함되지 않을 수 있습니다.

AWS::ApiGateway::Stage

Amazon API Gateway 버전 1단계.

- ARN 형식: `arn:partition:apigateway:region:account:/restapis/api-id/stages/stage-name`

  예제: `arn:aws:apigateway:us-east-1:111122223333:/restapis/123456789/stages/ExampleStage`

  자세한 내용은 API Gateway Amazon 리소스 이름(ARN) 참조를 참조하세요.

AWS::ApiGatewayV2::Stage

Amazon API Gateway 버전 2단계.

- ARN 형식: `arn:partition:apigateway:region:account:/apis/api-id/stages/stage-name`

  예제: `arn:aws:apigateway:us-east-1:111122223333:/apis/123456789/stages/ExampleStage`

  자세한 내용은 API Gateway Amazon 리소스 이름(ARN) 참조를 참조하세요.

AWS::CloudWatch::Alarm

아마존 CloudWatch 알람.

- ARN 형식: `arn:partition:cloudwatch:region:account:alarm:alarm-name`

예제: `arn:aws:cloudwatch:us-west-2:111122223333:alarm:test-alarm-1`

자세한 내용은 Amazon에서 정의한 리소스 유형을 참조하십시오 CloudWatch.

AWS::DynamoDB::Table

Amazon DynamoDB 테이블.

- ARN 형식: `arn:`*`partition`*`:dynamodb:`*`region`*`:`*`account`*`:table/`*`table-name`*

  예제: `arn:aws:dynamodb:us-west-2:111122223333:table/BigTable`

  자세한 내용은 DynamoDB 리소스 및 작업을 참조하세요.

AWS::EC2::CustomerGateway

고객 게이트웨이 디바이스.

- ARN 형식: `arn:`*`partition`*`:ec2:`*`region`*`:`*`account`*`:customer-gateway/`*`CustomerGatewayId`*

  예제: `arn:aws:ec2:us-west-2:111122223333:customer-gateway/vcg-123456789`

  자세한 정보는 Amazon EC2에 의해 정의된 리소스 유형을 참조하세요.

AWS::EC2::Volume

Amazon EBS 볼륨.

- ARN 형식: `arn:`*`partition`*`:ec2:`*`region`*`:`*`account`*`:volume/`*`VolumeId`*

  예제: `arn:aws:ec2:us-west-2:111122223333:volume/volume-of-cylinder-is-pi`

  자세한 내용은 API Gateway Amazon 리소스 이름(ARN) 참조를 참조하세요.

AWS::ElasticLoadBalancing::LoadBalancer

Classic Load Balancer.

- ARN 형식: `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account`*`:loadbalancer/`*`LoadBalancerN`

  예제: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/123456789abcbdeCLB`

  자세한 내용은 Elastic Load Balancing 리소스를 참조하세요.

AWS::ElasticLoadBalancingV2::LoadBalancer

Network Load Balancer 또는 Application Load Balancer.

- Network Load Balancer의 ARN 형식: `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Network Load Balancer의 예: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdeNLB`
- Application Load Balancer의 ARN 형식: `arn:partition:elasticloadbalancing:region:account:loadbalancer/app/LoadBalancerName`

  Application Load Balancer의 예: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/app/sandbox-alb/123456789acbdeALB`

  자세한 내용은 Elastic Load Balancing 리소스를 참조하세요.

AWS::Lambda::Function

AWS Lambda 함수.

- ARN 형식: `arn:partition:lambda:region:account:function:FunctionName`

  예제: `arn:aws:lambda:us-west-2:111122223333:function:my-function`

  자세한 내용은 Lambda 작업을 위한 리소스 및 조건을 참조하세요.

AWS::MSK::Cluster

Amazon MSK 클러스터.

- ARN 형식: `arn:partition:kafka:region:account:cluster/ClusterName/UUID`

  예제: `arn:aws:kafka:us-east-1:111122223333:cluster/demo-cluster-1/123456-1111-2222-3333`

  자세한 내용은 Amazon Managed Streaming for Apache Kafka에 의해 정의된 리소스 유형을 참조하세요.

AWS::RDS::DBCluster

Aurora DB 클러스터.

- ARN 형식: `arn:partition:rds:region:account:cluster:DbClusterInstanceName`

  예제: `arn:aws:rds:us-west-2:111122223333:cluster:database-1`

  자세한 내용은 Amazon RDS에서 Amazon 리소스 이름(ARN) 작업을 참조하세요.

AWS::Route53::HealthCheck

Amazon Route 53 상태 확인.

- ARN 형식: `arn:partition:route53:::healthcheck/Id`

  예제: `arn:aws:route53:::healthcheck/123456-1111-2222-3333`

AWS::SQS::Queue

Amazon SQS 대기열.

- ARN 형식: `arn:partition:sqs:region:account:QueueName`

  예제: `arn:aws:sqs:us-west-2:111122223333:StandardQueue`

  자세한 내용은 Amazon Simple Queue Service 리소스 및 작업을 참조하세요.

AWS::SNS::Topic

Amazon SNS 주제.

- ARN 형식: `arn:partition:sns:region:account:TopicName`

  예제: `arn:aws:sns:us-west-2:111122223333:TopicName`

  자세한 내용은 Amazon SNS 리소스 ARN 형식을 참조하세요.

AWS::SNS::Subscription

Amazon SNS 구독.

- ARN 형식: `arn:partition:sns:region:account:TopicName:SubscriptionId`

  예제: `arn:aws:sns:us-west-2:111122223333:TopicName:12345678901234567890`

AWS::EC2::VPC

Virtual Private Cloud(VPC).

- ARN 형식: `arn:partition:ec2:region:account:vpc/VpcId`

  예제: `arn:aws:ec2:us-west-2:111122223333:vpc/vpc-123456789`

자세한 내용은 VPC 리소스를 참조하세요.

AWS::EC2::VPNConnection

가상 프라이빗 네트워크(VPN) 연결.

- ARN 형식: `arn:partition:ec2:region:account:vpn-connection/VpnConnectionId`

  예제: `arn:aws:ec2:us-west-2:111122223333:vpn-connection/vpn-123456789`

  자세한 정보는 Amazon EC2에 의해 정의된 리소스 유형을 참조하세요.

AWS::EC2::VPNGateway

가상 프라이빗 네트워크(VPN) 게이트웨이.

- ARN 형식: `arn:partition:ec2:region:account:vpn-gateway/VpnGatewayId`

  예제: `arn:aws:ec2:us-west-2:111122223333:vpn-gateway/vgw-123456789acbdefgh`

  자세한 정보는 Amazon EC2에 의해 정의된 리소스 유형을 참조하세요.

AWS::Route53RecoveryReadiness::DNSTargetResource

준비 확인을 위한 DNS 대상 리소스에는 DNS 레코드 유형, 도메인 이름, Route 53 호스팅 영역 ARN, Network Load Balancer ARN 또는 Route 53 레코드 세트 ID가 포함됩니다.

- 호스팅 영역의 ARN 형식: `arn:partition:route53::account:hostedzone/Id`

  호스팅 영역의 예: `arn:aws:route53::111122223333:hostedzone/abcHostedZone`

  참고: 여기에 지정된 대로 호스팅 영역 ARN에 계정 ID를 포함해야 합니다. Route 53 ARC가 리소스를 폴링하려면 계정 ID가 필요합니다. 형식은 Amazon Route 53에서 요구하는 ARN 형식과 의도적으로 다릅니다. 이 형식은 서비스 권한 부여 참조의 Route 53 서비스 리소스 유형에 설명되어 있습니다.

- Network Load Balancer의 ARN 형식: `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Network Load Balancer의 예: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdefgh`

자세한 내용은 Elastic Load Balancing 리소스를 참조하세요.

Amazon Route 53 애플리케이션 복구 컨트롤러에서의 준비 상태 확인을 위한 로깅 및 모니터링

Amazon CloudWatch AWS CloudTrail, 및 Amazon을 사용하여 Amazon EventBridge Route 53 애플리케이션 복구 컨트롤러에서 준비 상태 확인을 모니터링하여 패턴을 분석하고 문제를 해결할 수 있습니다.

> **Note**
>
> 콘솔과 사용 시 모두 미국 서부 (오레곤) 지역의 Route 53 ARC에 대한 CloudWatch 메트릭과 로그를 확인해야 합니다. AWS CLI를 사용할 경우 다음 파라미터를 포함하여 명령에 사용할 미국 서부 (오레곤) 지역을 지정하십시오. AWS CLI`--region us-west-2`

주제

- Route 53 ARC에서 준비 상태 CloudWatch 확인과 함께 아마존 사용하기
- 를 사용하여 준비 상태 확인 API 호출 로깅 AWS CloudTrail
- Amazon에서 Route 53 ARC에서 준비 상태 확인 사용하기 EventBridge

Route 53 ARC에서 준비 상태 CloudWatch 확인과 함께 아마존 사용하기

Amazon Route 53 애플리케이션 복구 컨트롤러는 준비 상태 확인을 CloudWatch 위해 Amazon에 데이터 포인트를 게시합니다. CloudWatch 이러한 데이터 포인트에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 지표를 모니터링할 변수로 생각하면 데이터 요소는 시간에 따른 변수의 값을 나타냅니다. 예를 들어, 지정된 기간 동안 AWS 지역을 통과하는 트래픽을 모니터링할 수 있습니다. 각 데이터 요소에는 연결된 타임스탬프와 측정 단위(선택 사항)가 있습니다.

지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 예를 들어, 지정된 지표를 모니터링하는 CloudWatch 경보를 만들어 지표가 허용 범위를 벗어나는 경우 작업 (예: 이메일 주소로 알림 전송) 을 시작할 수 있습니다.

자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

주제

- Route 53 ARC 지표
- Route 53 RC 지표에 대한 통계
- Route 53 ARC에서 CloudWatch 메트릭을 확인하세요

Route 53 ARC 지표

AWS/Route53RecoveryReadiness 네임스페이스에 포함된 지표는 다음과 같습니다.

지표	설명
ReadinessChecks	Route 53 ARC에서 처리한 준비 확인 수를 나타냅니다. 지표는 아래 나열된 상태를 기준으로 측정할 수 있습니다. 단위: Count. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • READY • NOT_READY • NOT_AUTHORIZED • UNKNOWN
Resources	Route 53 ARC에서 처리한 리소스 수를 나타내며, API에서 정의한 리소스 식별자로 차원을 조정할 수 있습니다. 단위: Count. 보고 기준: 0이 아닌 값이 있을 때. 통계: 가장 유용한 통계는 Sum입니다. 차원 • ResourceSetType : Route 53 ARC에서 평가한 특정 유형별 리소스 수를 기준으로 필터링된 리소스 유형입니다.

지표	설명
	예: `AWS::CloudWatch::Alarm`

Route 53 RC 지표에 대한 통계

CloudWatch Route 53 ARC에서 게시한 지표 데이터 포인트를 기반으로 통계를 제공합니다. 통계는 지정한 기간에 걸친 지표 데이터 집계입니다. 통계를 요청하면 지표 이름 및 차원으로 반환된 데이터 스트림이 식별됩니다. 차원이란 지표를 고유하게 식별하는 데 도움이 되는 이름/값 쌍을 말합니다.

다음은 유용할 수 있는 지표/차원 조합의 예입니다.

- Route 53 ARC에서 준비를 평가한 준비 확인 수를 봅니다.
- Route 53 ARC에서 평가한 특정 리소스 세트 유형의 총 리소스 수를 확인합니다.

Route 53 ARC에서 CloudWatch 메트릭을 확인하세요

CloudWatch 콘솔 또는 를 사용하여 Route 53 ARC에 대한 CloudWatch 메트릭을 볼 수 AWS CLI있습니다. 콘설에서 지표는 모니터링 그래프로 표시됩니다.

콘솔에서 또는 를 사용할 때 미국 서부 (오레곤) 지역의 Route 53 ARC에 대한 CloudWatch 메트릭을 확인해야 합니다 AWS CLI. 를 사용할 경우 다음 파라미터를 포함하여 명령에 사용할 미국 서부 (오레곤) 지역을 지정하십시오. AWS CLI`--region us-west-2`

콘솔을 CloudWatch 사용하여 지표를 보려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표(Metrics)를 선택합니다.
3. Route53 RecoveryReadiness 네임스페이스를 선택합니다.
4. (선택 사항) 모든 차원의 지표를 보려면 검색 필드에 이름을 입력합니다.

를 사용하여 메트릭을 보려면 AWS CLI

사용 가능한 지표의 목록을 표시하려면 아래 list-metrics 명령을 사용하세요.

```
aws cloudwatch list-metrics --namespace AWS/Route53RecoveryReadiness --region us-west-2
```

를 사용하여 지표에 대한 통계를 가져오려면 AWS CLI

다음 get-metric-statistics명령을 사용하여 지정된 지표 및 차원에 대한 통계를 가져올 수 있습니다. 참고로 각 고유한 측정기준 조합은 별도의 지표로 CloudWatch 취급됩니다. 특별 게시가 되지 않은 차원의 조합을 사용해 통계를 검색할 수는 없습니다. 지표 생성 시 사용한 것과 동일하게 차원을 지정해야 합니다.

다음 예는 Route 53 ARC에 있는 계정에 대해 분당 평가된 총 준비 확인을 나열합니다.

```
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
```

다음은 명령의 출력 예제입니다.

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

를 사용하여 준비 상태 확인 API 호출 로깅 AWS CloudTrail

Amazon Route 53 애플리케이션 복구 컨트롤러는 Route 53 ARC에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 기록을 제공하는 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail Route 53 ARC에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Route 53 ARC 콘솔로부터의 호출과 Route 53 ARC API 작업에 대한 코드 호출이 포함됩니다.

트레일을 생성하면 Route 53 ARC에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷에 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다.

에서 수집한 CloudTrail 정보를 사용하여 Route 53 ARC에 대한 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Route 53 ARC 정보는 다음과 같습니다. CloudTrail

CloudTrail 계정을 생성할 AWS 계정 때 활성화됩니다. Route 53 ARC에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 CloudTrail 이벤트 기록 작업을 참조하십시오.

Route 53 ARC에 대한 이벤트를 AWS 계정포함하여 귀하의 이벤트에 대한 지속적인 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Route 53 ARC 작업은 Amazon Route 53 애플리케이션 복구 컨트롤러용 복구 준비 API 참조 가이드, Amazon Route 53 애플리케이션 복구 컨트롤러용 복구 제어 구성 API 참조 가이드, Amazon Route 53 애플리케이션 복구 컨트롤러용 라우팅 제어 API 참조 가이드에 의해 CloudTrail 기록되고 문서화됩니다. 예를 들어`CreateCluster`, 에 대한 호출 `UpdateRoutingControlState` 및 `CreateRecoveryGroup` 작업은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail 사용자 ID 요소를 참조하십시오.

이벤트 기록에서 Route 53 ARC 이벤트 확인하기

CloudTrail 이벤트 기록에서 최근 이벤트를 볼 수 있습니다. Route 53 ARC API 요청에 대한 이벤트를 확인하려면 콘솔 상단의 리전 선택기에서 미국 서부(오레곤)를 선택해야 합니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록 작업을 참조하십시오.

Route 53 ARC 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일은 하나 이상의 로그 항목을 포함합니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 준비 상태 확인 `CreateRecoveryGroup` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "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"
}
```

Amazon에서 Route 53 ARC에서 준비 상태 확인 사용하기 EventBridge

Amazon을 사용하면 Amazon EventBridge Route 53 애플리케이션 복구 컨트롤러에서 준비 상태 확인 리소스를 모니터링하는 이벤트 기반 규칙을 설정한 다음 다른 서비스를 사용하는 대상 작업을 시작할 수 있습니다. AWS 예를 들어, 준비 상태 확인 상태가 READY에서 NOT READY로 변경될 때 Amazon SNS 주제에 신호를 보내 이메일 알림을 보내는 규칙을 설정할 수 있습니다.

> **Note**
>
> Route 53 ARC는 미국 서부 (오레곤) (us-west-2) 지역의 준비 상태 확인을 위한 EventBridge 이벤트만 게시합니다. AWS 준비 상태 점검을 위한 EventBridge 이벤트를 수신하려면 미국 서부 (오레곤) 지역에서 EventBridge 규칙을 생성하십시오.

Amazon에서 규칙을 EventBridge 생성하여 다음과 같은 Route 53 ARC 준비 상태 확인 이벤트에 대해 조치를 취할 수 있습니다.

- 준비 확인 준비. 이벤트는 준비 확인 상태가 변경되는지 여부를 지정합니다(예: READY에서 NOT READY로).

관심 있는 특정 Route 53 ARC 이벤트를 캡처하려면 이벤트 감지에 사용할 EventBridge 수 있는 이벤트별 패턴을 정의하십시오. 이벤트 패턴은 일치하는 이벤트와 동일한 구조를 갖습니다. 패턴은 일치시키려는 필드를 인용하고 찾고 있는 값을 제공합니다.

이벤트는 최선의 작업을 기반으로 발생됩니다. 정상적인 운영 EventBridge 환경에서는 Route 53 ARC에서 거의 실시간으로 전송됩니다. 하지만 이벤트 전달을 지연하거나 방해하는 상황이 발생할 수 있습니다.

EventBridge 규칙이 이벤트 패턴과 함께 작동하는 방식에 대한 자세한 내용은 의 이벤트 및 이벤트 패턴을 참조하십시오 EventBridge.

다음을 통해 준비 상태 확인 리소스를 모니터링하십시오. EventBridge

를 사용하면 Route 53 ARC가 준비 확인 리소스에 대한 이벤트를 내보낼 때 취할 조치를 정의하는 규칙을 생성할 수 있습니다. EventBridge

이벤트 패턴을 EventBridge 콘솔에 입력하거나 복사하여 붙여넣으려면 콘솔에서 내 옵션 입력 옵션을 선택합니다. 자신에게 유용할 수 있는 이벤트 패턴을 쉽게 파악할 수 있도록 이 항목에는 준비 이벤트 패턴의 예시가 포함되어 있습니다.

리소스 이벤트에 대한 규칙을 만들려면

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 에서 규칙을 AWS 리전 생성하려면 미국 서부 (오레곤) 를 선택하십시오. 준비 이벤트에 필요한 지역입니다.
3. Create rule을 선택합니다.
4. 규칙의 이름을 입력하고 선택적으로 설명을 입력합니다.
5. 이벤트 버스의 경우 기본값을 그대로 두세요.
6. 다음을 선택합니다.
7. 이벤트 패턴 빌드 단계에서 이벤트 소스의 경우 기본값인 AWS 이벤트를 그대로 두세요.
8. 샘플 이벤트에서 직접 입력을 선택합니다.
9. 샘플 이벤트에 이벤트 패턴을 입력하거나 복사하여 붙여넣습니다. 예를 들어 다음 섹션을 참조하십시오.

준비 이벤트 패턴 예시

이벤트 패턴은 일치하는 이벤트와 동일한 구조를 갖습니다. 패턴은 일치시키려는 필드를 인용하고 찾고 있는 값을 제공합니다.

이 섹션의 이벤트 패턴을 복사하여 붙여넣어 Route 53 ARC 작업 및 리소스를 모니터링하는 데 사용할 수 있는 규칙을 생성할 수 있습니다. EventBridge

다음 이벤트 패턴은 Route 53 ARC의 준비 확인 기능에 사용할 수 있는 예를 제공합니다. EventBridge

- Route 53 ARC 준비 확인에서 모든 이벤트를 선택합니다.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ]
}
```

- 셀과 관련된 이벤트만 선택합니다.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
```

```
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ]
}
```

- MyExampleCell이라는 특정 셀과 관련된 이벤트만 선택합니다.

```
{
    "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"
    ]
}
```

- 복구 그룹, 셀 또는 준비 확인 상태가 NOT READY인 경우에만 이벤트를 선택합니다.

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail-type":{
      "new-state":{
         "readiness-status":[
            "NOT_READY"
         ]
      }
   }
}
```

- 복구 그룹, 셀 또는 준비 확인이 READY가 아닌 경우에만 이벤트를 선택합니다.

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail":{
      "new-state":{
         "readiness-status":[
```

```
            {
               "anything-but":"READY"
            }
         ]
      }
   }
}
```

다음은 복구 그룹 준비 상태 변경에 대한 Route 53 ARC 이벤트의 예입니다.

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

다음은 셀 준비 상태 변경에 대한 Route 53 ARC 이벤트의 예입니다.

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

다음은 준비 확인 상태 변경에 대한 Route 53 ARC 이벤트의 예입니다.

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

대상으로 사용할 CloudWatch 로그 그룹을 지정합니다.

규칙을 생성할 때는 EventBridge 규칙과 일치하는 이벤트가 전송되는 대상을 지정해야 합니다. 사용 가능한 대상 EventBridge 목록은 EventBridge 콘솔에서 사용 가능한 대상을 참조하십시오. EventBridge 규칙에 추가할 수 있는 대상 중 하나는 Amazon CloudWatch 로그 그룹입니다. 이 섹션에서는 CloudWatch 로그 그룹을 대상으로 추가하기 위한 요구 사항을 설명하고 규칙을 생성할 때 로그 그룹을 추가하는 절차를 제공합니다.

CloudWatch 로그 그룹을 대상으로 추가하려면 다음 중 하나를 수행할 수 있습니다.

- 새 로그 그룹 생성
- 기존 로그 그룹 선택

규칙을 생성할 때 콘솔을 사용하여 새 로그 그룹을 지정하면 이 EventBridge 자동으로 로그 그룹을 생성합니다. EventBridge 규칙의 대상으로 사용하는 로그 그룹이 로 시작하는지 확인하십시오`/aws/events`. 기존 로그 그룹을 선택하려는 경우 로 시작하는 로그 그룹만 드롭다운 메뉴에 옵션으로 `/aws/events` 표시된다는 점에 유의하세요. 자세한 내용은 Amazon CloudWatch 사용 설명서의 새 로그 그룹 생성을 참조하십시오.

콘솔 외부의 CloudWatch 작업을 사용하여 대상으로 사용할 CloudWatch 로그 그룹을 만들거나 사용하는 경우 권한을 올바르게 설정해야 합니다. 콘솔을 사용하여 EventBridge 규칙에 로그 그룹을 추가하면 해당 로그 그룹의 리소스 기반 정책이 자동으로 업데이트됩니다. 그러나 AWS Command Line Interface 또는 AWS SDK를 사용하여 로그 그룹을 지정하는 경우 로그 그룹에 대한 리소스 기반 정책을 업데이트해야 합니다. 다음 예제 정책은 리소스 기반 정책에서 로그 그룹에 정의해야 하는 권한을 보여줍니다.

```
{
  "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"
}
```

콘솔을 사용하여 로그 그룹에 대한 리소스 기반 정책을 구성할 수는 없습니다. 리소스 기반 정책에 필요한 권한을 추가하려면 Policy API 작업을 사용하십시오. CloudWatch PutResource 그런 다음 describe-resource-policy CLI 명령을 사용하여 정책이 올바르게 적용되었는지 확인할 수 있습니다.

리소스 이벤트에 대한 규칙을 생성하고 로그 그룹 대상을 지정하려면 CloudWatch

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 규칙을 AWS 리전 생성하려는 항목을 선택합니다.
3. 규칙 생성을 선택한 다음 해당 규칙에 대한 정보 (예: 이벤트 패턴 또는 일정 세부 정보) 를 입력합니다.

   준비 상태를 위한 EventBridge 규칙을 만드는 방법에 대한 자세한 내용은 다음을 사용하여 준비 상태 확인 리소스 모니터링을 참조하십시오. EventBridge
4. 대상 선택 페이지에서 CloudWatch대상으로 선택합니다.
5. 드롭다운 메뉴에서 CloudWatch 로그 그룹을 선택합니다.

준비 상태 확인을 위한 Identity 및 Access Management

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 누가 Route 53 ARC 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

내용

- ServiceLong; 의 준비 상태 확인이 IAM과 함께 작동하는 방식
- Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인을 위한 ID 기반 정책 예제
- Route 53 ARC에서 준비 상태 확인을 위한 서비스 연결 역할 사용
- AWS Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인을 위한 관리형 정책

ServiceLong; 의 준비 상태 확인이 IAM과 함께 작동하는 방식

IAM을 사용하여 Route 53 ARC에 대한 액세스를 관리하기 전에 Route 53 ARC와 함께 사용할 수 있는 IAM 기능을 알아봅니다.

Amazon Route 53 애플리케이션 복구 컨트롤러에서 IAM을 사용하여 준비 상태 확인에 대한 액세스를 관리하기 전에 준비 확인과 함께 사용할 수 있는 IAM 기능에 대해 알아보십시오.

Amazon Route 53 애플리케이션 복구 컨트롤러에서 준비 상태 확인과 함께 사용할 수 있는 IAM 기능

IAM 특성	준비 확인 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 링크 역할	예

AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 개괄적으로 파악하려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

준비 상태 확인을 위한 ID 기반 정책

ID 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Route 53 ARC 자격 증명 기반 정책의 예를 보려면 Amazon Route 53 애플리케이션 복구 컨트롤러의 ID 기반 정책 예제 섹션을 참조하세요.

준비 상태 점검 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다.

준비 상태 점검을 위한 정책 조치

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

준비 상태 확인을 위한 Route 53 ARC 작업 목록을 보려면 서비스 권한 부여 참조의 Amazon Route 53 복구 준비에 의해 정의된 작업을 참조하십시오.

준비 상태 확인을 위한 Route 53 ARC의 정책 조치는 조치 전에 다음 접두사를 사용합니다.

```
route53-recovery-readiness
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다. 예를 들면 다음과 같습니다.

```
"Action": [
      "route53-recovery-readiness:action1",
      "route53-recovery-readiness:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Describe라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "route53-recovery-readiness:Describe*"
```

준비 상태 확인을 위한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인을 위한 ID 기반 정책 예제

준비 상태 확인을 위한 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

영역 이동에 대한 Route 53 ARC 작업 목록을 보려면 Amazon Route 53 복구 준비에서 정의한 작업을 참조하십시오.

준비 상태 확인을 위한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인을 위한 ID 기반 정책 예제

준비 상태 검사를 위한 정책 조건 키

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition`요소를 지정하거나 단일 `Condition`요소에서 여러 키를 지정하는 경우 AWS 는 논리적 `AND`태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

준비 상태 확인을 위한 Route 53 ARC 작업 목록을 보려면 Amazon Route 53 복구 준비 상태를 위한 조건 키를 참조하십시오.

준비 상태 확인과 함께 조건 키와 함께 사용할 수 있는 작업 및 리소스를 보려면 Amazon Route 53에서 정의한 작업 복구 준비를 참조하십시오.

준비 상태 확인을 위한 Route 53 ARC ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인을 위한 ID 기반 정책 예제

준비 상태 확인의 액세스 제어 목록 (ACL)

ACL 지원	아니요

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

준비 상태 확인을 포함한 속성 기반 액세스 제어 (ABAC)

ABAC(정책 내 태그) 지원	부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

복구 준비 상태 (준비 확인) 는 ABAC를 지원합니다.

준비 상태 확인과 함께 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 일부 자격 증명이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다

음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

준비 상태 확인을 위한 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원	예

IAM 개체 (사용자 또는 역할) 를 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 정책은 보안 주체에게 권한을 부여합니다. 일부 서비스를 사용할 때는 다른 서비스에서 다른 작업을 트리거하는 작업을 수행할 수 있습니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다.

준비 상태 확인 중인 작업에 정책의 종속 작업이 추가로 필요한지 확인하려면 Amazon Route 53 복구 준비를 참조하십시오.

준비 상태 확인을 위한 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조합니다.

준비 상태 확인을 위한 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Route 53 ARC 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 Route 53 ARC에서 준비 상태 확인을 위한 서비스 연결 역할 사용 섹션을 참조하세요.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스 단원을 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인을 위한 ID 기반 정책 예제

기본적으로 사용자 및 역할에는 Route 53 ARC 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 API를 사용하여 작업을 수행할 수 없습니다. AWS 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 비롯하여 Route 53 ARC에 의해 정의되는 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 Amazon Route 53 Application Recovery Controller에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- 예: 준비 상태 확인 콘솔 액세스
- 예: 준비 상태 확인을 위한 준비 확인 API 작업

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Route 53 ARC 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있

는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.

- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

예: 준비 상태 확인 콘솔 액세스

Amazon Route 53 Application Recovery Controller 콘솔에 액세스하려면 최소한의 권한 세트가 있어야 합니다. 이러한 권한을 통해 내 Route 53 ARC 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

특정 API 작업에만 액세스를 허용할 때 사용자와 역할이 준비 검사 콘솔을 계속 사용할 수 있도록 하려면 준비 상태 검사를 위한 `ReadOnly` AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 준비 상태 검사 준비 검사 관리형 정책 페이지 또는 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

일부 작업을 수행하려면 사용자에게 Route 53 ARC에서 준비 상태 확인과 관련된 서비스 연결 역할을 생성할 수 있는 권한이 있어야 합니다. 자세한 내용은 Route 53 ARC에서 준비 상태 확인을 위한 서비스 연결 역할 사용 섹션을 참조하세요.

사용자에게 콘솔을 통해 준비 상태 확인 기능을 사용할 수 있는 전체 액세스 권한을 부여하려면 다음과 같은 정책을 사용자에게 연결하십시오.

```
{
    "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": "*"
        }
    ]
}
```

예: 준비 상태 확인을 위한 준비 확인 API 작업

사용자가 Route 53 ARC 준비 상태 검사 컨트롤 플레인을 사용하여 Route 53 ARC 준비 상태 검사 컨트롤 플레인을 사용할 수 있도록 하려면 (예: 복구 그룹, 리소스 세트, 준비 검사 생성) 사용자가 작업해야 하는 API 작업에 해당하는 정책을 아래에 설명된 대로 연결하십시오.

일부 작업을 수행하려면 사용자에게 Route 53 ARC에서 준비 상태 확인과 관련된 서비스 연결 역할을 생성할 수 있는 권한이 있어야 합니다. 자세한 내용은 Route 53 ARC에서 준비 상태 확인을 위한 서비스 연결 역할 사용 섹션을 참조하세요.

준비 상태 확인을 위한 API 작업을 수행하려면 다음과 같은 정책을 사용자에게 연결하십시오.

```
{
    "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": "*"
        }
    ]
}
```

Route 53 ARC에서 준비 상태 확인을 위한 서비스 연결 역할 사용

Amazon Route 53 애플리케이션 복구 컨트롤러는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 서비스(이 경우에는 Route 53 ARC)에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Route 53 ARC에 의해 사전 정의되며, 서비스가 특정 목적을 위해 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할을 사용하면 Route 53 ARC를 더 쉽게 설정할 수 있습니다. Route 53 ARC에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Route 53 ARC만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Route 53 ARC 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 표시된 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Route 53 ARC에는 이 챕터에 설명된 다음과 같은 서비스 연결 역할이 있습니다.

- Route53 ARC는 Route53이라는 서비스 연결 역할을 사용하여 리소스와 구성에 RecoveryReadinessServiceRolePolicy 액세스하여 준비 상태를 확인합니다.
- Route 53 ARC는 자동 전환 연습 실행을 위해 이름이 지정된 서비스 연결 역할을 사용하여 고객이 제공한 Amazon CloudWatch 경보 및 고객 AWS Health Dashboard 이벤트를 모니터링하고 연습 실행을 시작합니다.

Route53에 대한 서비스 연결 역할 권한 RecoveryReadinessServiceRolePolicy

Route53 ARC는 Route53이라는 서비스 연결 역할을 사용하여 리소스와 구성에 RecoveryReadinessServiceRolePolicy 액세스하여 준비 상태를 확인합니다. 이 섹션에서는 서비스 연결 역할에 대한 권한과 역할 생성, 편집 및 삭제에 대한 정보를 설명합니다.

Route53에 대한 서비스 연결 역할 권한 RecoveryReadinessServiceRolePolicy

서비스 연결 역할은 관리형 정책 `Route53RecoveryReadinessServiceRolePolicy`를 사용합니다.

Route53 RecoveryReadinessServiceRolePolicy 서비스 연결 역할은 다음 서비스가 역할을 맡을 것으로 신뢰합니다.

- `route53-recovery-readiness.amazonaws.com`

이 정책에 대한 권한을 보려면 관리형 정책 참조의 RecoveryReadinessServiceRolePolicyRoute53을 참조하십시오.AWS

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Route53 ARC에 대한 Route53 RecoveryReadinessServiceRolePolicy 서비스 연결 역할 생성

Route53 서비스 연결 역할을 수동으로 생성할 필요는 없습니다. RecoveryReadinessServiceRolePolicy AWS Management Console, 또는 AWS API에서 첫 번째 준비 상태 확인 또는 교차 계정 인증을 생성하면 Route 53 ARC가 서비스 연결 역할을 생성합니다. AWS CLI

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 첫 번째 준비 확인 또는 크로스 계정 권한 부여를 생성할 때 Route 53 ARC는 서비스 연결 역할을 다시 생성합니다.

Route53 ARC에 대한 Route53 RecoveryReadinessServiceRolePolicy 서비스 연결 역할 편집

Route53 ARC에서는 Route53 RecoveryReadinessServiceRolePolicy 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다른 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Route53 ARC에 대한 Route53 RecoveryReadinessServiceRolePolicy 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

준비 상태 확인 및 교차 계정 인증을 제거한 후에는 Route53 서비스 연결 역할을 삭제할 수 있습니다. RecoveryReadinessServiceRolePolicy 준비 확인에 대한 자세한 내용은 Amazon Route 53 Application Recovery Controller의 준비 확인 섹션을 참조하세요. 크로스 계정 권한 부여에 대한 자세한 내용은 Route 53 ARC에서 교차 계정 권한 생성 섹션을 참조하세요.

> **Note**
>
> 리소스를 삭제하려 할 때 Route 53 ARC 서비스가 역할을 사용 중이면 서비스 역할 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 역할 삭제를 다시 시도하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔 AWS CLI, 또는 API를 사용하여 Route53 서비스 연결 역할을 삭제하십시오. AWS RecoveryReadinessServiceRolePolicy 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

준비 상태 확인을 위한 Route 53 ARC 서비스 연결 역할 업데이트

Route 53 ARC 서비스 연결 역할의 AWS 관리형 정책 업데이트는 Route 53 ARC의AWS 관리형 정책 업데이트 표를 참조하십시오. Route 53 ARC 문서 기록 페이지에서 자동 RSS 알림을 구독할 수도 있습니다.

AWS Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인을 위한 관리형 정책

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: Route53 RecoveryReadinessServiceRolePolicy

`Route53RecoveryReadinessServiceRolePolicy`를 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Route 53 ARC에서 사용하거나 관리하는 AWS 서비스 및 리소스에 Amazon Route 53 Application Recovery Controller가 액세스할 수 있는 서비스 연결 역할에 연결됩니다. 자세한 정보는 Route 53 ARC에서 준비 상태 확인을 위한 서비스 연결 역할 사용을 참조하세요.

AWS 관리형 정책: 53 AmazonRoute RecoveryReadinessFullAccess

`AmazonRoute53RecoveryReadinessFullAccess`를 IAM 엔터티에 연결할 수 있습니다. 이 정책은 Route 53 ARC에서 복구 준비(준비 확인) 작업에 대한 전체 액세스 권한을 부여합니다. 복구 준비 작업에 대한 전체 액세스가 필요한 IAM 사용자 및 다른 보안 주체에 이 정책을 연결합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 RecoveryReadinessFullAccess 참조의 AmazonRoute 53을 참조하십시오.

AWS 관리형 정책: AmazonRoute 53 RecoveryReadinessReadOnlyAccess

`AmazonRoute53RecoveryReadinessReadOnlyAccess`를 IAM 엔터티에 연결할 수 있습니다. 이 정책은 Route 53 ARC에서 복구 준비 작업에 대한 읽기 전용 액세스 권한을 부여합니다. 준비 상태 및 복구 그룹 구성을 확인해야 하는 사용자에게 유용합니다. 이러한 사용자는 복구 준비 리소스를 생성, 업데이트 또는 삭제할 수 없습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 RecoveryReadinessReadOnlyAccess 참조의 AmazonRoute 53을 참조하십시오.

준비를 위한 AWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Route 53 ARC의 준비 상태 확인을 위한 AWS 관리형 정책 업데이트에 대한 자세한 내용은 을 참조하십시오Amazon Route 53 애플리케이션 복구 컨트롤러의 AWS 관리형 정책 업데이트. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 Route 53 ARC 문서 기록 페이지에서 RSS 피드를 구독합니다.

준비 상태 확인을 위한 할당량

Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 검사에는 다음과 같은 할당량 (이전에는 한도라고 함) 이 적용됩니다.

개체	할당량
계정당 복구 그룹 수	5
계정당 셀 수	15
셀당 중첩된 셀 수	3
복구 그룹당 셀 수	3
셀당 리소스 수	10
복구 그룹당 리소스 수	10
리소스 세트당 리소스 수	6
계정당 리소스 세트 수	200
계정당 준비 확인 수	200
크로스 계정 인증 수	100

AWS SDK를 사용하는 애플리케이션 복구 컨트롤러의 코드 예제

다음 코드 예제는 AWS 소프트웨어 개발 키트 (SDK) 와 함께 애플리케이션 복구 컨트롤러를 사용하는 방법을 보여줍니다.

작업은 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 작업은 개별 서비스 함수를 호출하는 방법을 보여 주며 관련 시나리오와 교차 서비스 예시에서 컨텍스트에 맞는 작업을 볼 수 있습니다.

AWS SDK 개발자 가이드의 전체 목록과 코드 예제는 을 참조하십시오. AWS SDK와 함께 이 서비스 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

코드 예시

- SDK를 사용하는 AWS 애플리케이션 복구 컨트롤러의 작업
  - AWS SDK 또는 GetRoutingControlState CLI와 함께 사용
  - AWS SDK 또는 UpdateRoutingControlState CLI와 함께 사용

SDK를 사용하는 AWS 애플리케이션 복구 컨트롤러의 작업

다음 코드 예제는 AWS SDK를 사용하여 개별 애플리케이션 복구 컨트롤러 작업을 수행하는 방법을 보여줍니다. 이들 발췌문은 애플리케이션 복구 컨트롤러 API를 호출하며, 컨텍스트에서 실행되어야 하는 더 큰 프로그램에서 발췌한 코드입니다. 각 예제에는 코드 설정 및 실행 지침을 찾을 수 있는 링크가 포함되어 있습니다. GitHub

다음 예제에는 가장 일반적으로 사용되는 작업만 포함되어 있습니다. 전체 목록은 Amazon Route 53 Application Recovery Controller API 참조를 참조하세요.

예제

- AWS SDK 또는 GetRoutingControlState CLI와 함께 사용
- AWS SDK 또는 UpdateRoutingControlState CLI와 함께 사용

AWS SDK 또는 **GetRoutingControlState** CLI와 함께 사용

다음 코드 예제는 `GetRoutingControlState`의 사용 방법을 보여줍니다.

Java

SDK for Java 2.x

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    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;
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API GetRoutingControlState참조를 참조하십시오.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 다음과 같습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
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
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 GetRoutingControlState.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SDK와 함께 이 서비스 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 **UpdateRoutingControlState** CLI와 함께 사용

다음 코드 예제는 UpdateRoutingControlState의 사용 방법을 보여줍니다.

Java

SDK for Java 2.x

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    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;
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API [UpdateRoutingControlState](참조를 참조하십시오.)

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 다음과 같습니다 GitHub. [AWS 코드 예제 리포지토리](에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.)

```
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)
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 UpdateRoutingControlState.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SDK와 함께 이 서비스 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

Amazon Route 53 Application Recovery Controller의 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처를 활용할 수 있습니다.

보안은 기업과 기업 간의 공동 책임입니다. AWS 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. Amazon Route 53 애플리케이션 복구 컨트롤러에 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램별 범위 내 서비스 규정 준수 참조하십시오.
- 클라우드에서의 보안 — 사용하는 AWS 서비스에 따라 책임이 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Route 53 ARC 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Route 53 ARC를 구성하는 방법을 보여줍니다. 또한 Route 53 ARC 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

Amazon Route 53 Application Recovery Controller의 데이터 보호

AWS 공동 책임 모델 Amazon Route 53 애플리케이션 복구 컨트롤러의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 은 (는) 모두를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터

프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔 AWS CLI, API 또는 AWS 서비스 AWS SDK를 사용하여 Route 53 ARC 또는 다른 것으로 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

저장된 데이터 암호화

고객 구성 정보는 서비스 소유의 Amazon DynamoDB 글로벌 테이블에 저장되며 저장 시 암호화됩니다.

Route 53 ARC 클러스터의 셀 상태를 포함하는 데이터 세트는 백업을 위해 Amazon EBS 볼륨에 기록됩니다. Route 53 ARC는 데이터가 유휴 상태일 때 기본 Amazon EBS 암호화를 사용합니다.

전송 중 암호화

Route 53 ARC 구성, 준비 상태 쿼리, 셀 상태 업데이트 등에 대한 고객 요청 및 응답은 TLS를 사용하여 서비스 전체에서 전송 중에 암호화됩니다.

Amazon Route 53 Application Recovery Controller용 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 도구입니다. AWS IAM 관리자는 누가 Route 53 ARC 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

고객

Route 53 ARC에서 수행하는 작업에 따라 사용 방법 AWS Identity and Access Management (IAM) 이 다릅니다.

서비스 사용자 - Route 53 ARC 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증 정보와 권한을 관리자가 제공합니다. 더 많은 Route 53 ARC 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Route 53 ARC의 기능에 액세스할 수 없는 경우 Amazon Route 53 Application Recovery Controller 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 - 회사에서 Route 53 ARC 리소스를 책임지고 있는 경우 Route 53 ARC에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Route 53 ARC 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Route 53 ARC에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Amazon Route 53 애플리케이션 복구 컨트롤러 기능이 IAM과 함께 작동하는 방식 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Route 53 ARC에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Route 53 ARC 자격 증명 기반 정책 예제를 보려면 Amazon Route 53 애플리케이션 복구 컨트롤러의 ID 기반 정책 예제 섹션을 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 연동 자격 증명으로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페

더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

연동 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 연동 자격 증명에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입

니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예컨대, 어떤 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자

또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole`태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 보안 인증 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

Amazon Route 53 애플리케이션 복구 컨트롤러 기능이 IAM과 함께 작동하는 방식

각 Amazon Route 53 애플리케이션 복구 컨트롤러 기능이 IAM과 함께 작동하는 방식에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 영역 이동을 위한 IAM
- 존 오토시프트를 위한 IAM
- 라우팅 제어를 위한 IAM
- 준비 상태 확인을 위한 IAM

Amazon Route 53 애플리케이션 복구 컨트롤러의 ID 기반 정책 예제

Amazon Route 53 애플리케이션 복구 컨트롤러의 각 기능에 대한 ID 기반 정책 예제를 보려면 각 기능에 대한 각 AWS Identity and Access Management 장의 다음 주제를 참조하십시오.

- 영역 자동 전환에 대한 ID 기반 정책 예제
- Amazon Route 53 애플리케이션 복구 컨트롤러의 영역 이동에 대한 ID 기반 정책 예제
- Amazon Route 53 애플리케이션 복구 컨트롤러의 라우팅 제어를 위한 ID 기반 정책 예제
- Amazon Route 53 애플리케이션 복구 컨트롤러의 준비 상태 확인을 위한 ID 기반 정책 예제

AWS Amazon Route 53 애플리케이션 복구 컨트롤러에 대한 관리형 정책

서비스 연결 역할에 대한 AWS 관리형 정책을 포함하여 관리형 정책이 포함된 Amazon Route 53 애플리케이션 복구 컨트롤러 기능의 관리형 정책에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 영역 자동 전환에 대한 관리형 정책
- 라우팅 제어를 위한 관리형 정책
- 준비 상태 확인을 위한 관리형 정책

Amazon Route 53 애플리케이션 복구 컨트롤러의 AWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Route 53 ARC의 기능에 대한 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 Route 53 ARC 문서 기록 페이지에서 RSS 피드를 구독합니다.

변경 사항	설명	날짜
AWSServiceRoleForPercPracticePolicy— 새 정책	Route 53에 자동 전환 및 연습 실행을 위한 새로운 서비스 연결 역할을 추가했습니다. Route 53 ARC는 서비스 연결 역할을 통해 활성화된 권한을 사용하여 고객이 제공한 CloudWatch Amazon 경보와 AWS Health Dashboard 고객 이벤트를 모니터링하여 실습 실행을 시작합니다. 새로운 서비스 연결 역할에 대한 자세한 내용은 에 대한 서비스 연결 역할 권한 AWSServiceRoleForZonalAutoshiftPracticeRun 섹션을 참조하세요.	2023년 11월 30일
AmazonRouteRecoveryControlConfigReadOnlyAccess53 — 업데이트된 정책	공유 AWS Resource Access Manager 리소스의 리소스 정책에 대한 `GetResourcePolicy` 세부 정보 반환을 지원하기 위해 에 대한 권한을 추가합니다.	2023년 10월 18일
Route53 RecoveryReadinessServiceRole 정책 — 업데이트된 정책	Route 53 ARC는 Amazon EC2 인스턴스에 대한 정보를 쿼리할 수 있는 새로운 권한을 추가했습니다. Route 53 ARC는 다음 권한을 사용하여 Amazon EC2 인스턴스 폴링을 지원하고, 준비 확인를 실행하며, 인스턴스의 준비 상태를 판단합니다.	2023년 2월 17일

변경 사항	설명	날짜

	`ec2:DescribeVpnGateways`
	
	`ec2:DescribeCustomerGateways`	

Route53 정책 — 업데이트된 정책 RecoveryReadinessServiceRole	Route 53 ARC는 Lambda 함수에 대한 정보를 쿼리할 수 있는 새로운 권한을 추가했습니다. Route 53 ARC는 다음 권한을 사용하여 Lambda 함수에 대한 정보를 쿼리해 준비 확인을 실행하고 함수의 준비 상태를 판단합니다. `lambda:ListProvisionedConcurrencyConfigs`	2022년 8월 31일
AmazonRoute53 RecoveryControl ConfigFull 액세스 — 업데이트된 정책	정책에서 Amazon Route 53 권한을 제거하고 선택적 권한을 나열한 메모를 추가했습니다.	2022년 5월 26일
AmazonRoute53 RecoveryControl ConfigFull 액세스 — 정책 업데이트	누락된 필수 Amazon Route 53 권한을 정책에 추가했습니다.	2022년 4월 15일
AmazonRoute53 RecoveryCluster ReadOnly 액세스 — 정책 업데이트	Route 53 ARC는 고가용성으로 라우팅 제어 ARN을 나열할 수 있는 새 권한 `route53-recovery-cluster:ListRoutingControls` 를 추가했습니다.	2022년 3월 15일

변경 사항	설명	날짜
AmazonRoute53 RecoveryControl ConfigRead OnlyAccess — 업데이트된 정책	Route 53 ARC는 리소스의 태그를 나열할 수 있는 새 권한 `route53-recovery-control-config:ListTagsForResources` 을 추가했습니다.	2021년 12월 20일
Route53 RecoveryReadiness ServiceRole 정책 — 업데이트된 정책	Route 53 ARC는 Amazon API Gateway에 대한 정보를 쿼리할 수 있는 새 권한을 추가했습니다. Route 53 ARC는 `apigateway:GET` 권한을 사용하여 API Gateway에 대한 정보를 쿼리해 준비 확인을 실행하고 준비 상태를 판단합니다.	2021년 10월 28일
AmazonRoute53 RecoveryReadiness ReadOnly 액세스 — 새 권한 추가	Route 53 ARC는 53 RecoveryReadinessReadOnlyAccess에 AmazonRoute 두 개의 새로운 권한을 추가했습니다. Route 53 ARC는 `route53-recovery-readiness:GetArchitectureRecommendations` 및 `route53-recovery-readiness:GetCellReadinessSummary` 를 사용하여 복구 준비 작업에 대한 읽기 전용 액세스를 허용합니다.	2021년 10월 15일

변경 사항	설명	날짜

Route53 RecoveryReadiness ServiceRole 정책 — 업데이트된 정책	Route 53 ARC는 Lambda 함수에 대한 정보를 쿼리할 수 있는 새로운 권한을 추가했습니다.
	
	Route 53 ARC는 다음 권한을 사용하여 Lambda 함수에 대한 정보를 쿼리해 준비 확인을 실행하고 해당 함수의 준비 상태를 판단합니다.
	
	`lambda:GetFunctionConcurrency`
	
	`lambda:GetFunctionConfiguration`
	
	`lambda:GetProvisionedConcurrencyConfig`
	
	`lambda:ListAliases`
	
	`lambda:ListVersionsByFunction`
	
	`lambda:ListEventSourceMappings`
	
	`lambda:ListFunctions`
		2021년 10월 8일

변경 사항	설명	날짜
Route53 RecoveryReadiness ServiceRole 정책 — 새로운 관리형 정책 추가	Route 53 ARC는 다음과 같은 새로운 관리형 정책을 추가했습니다. AmazonRoute53 RecoveryReadiness FullAccess AmazonRoute53 RecoveryReadiness ReadOnly 액세스 AmazonRoute53 RecoveryCluster FullAccess AmazonRoute53 RecoveryCluster ReadOnly 액세스 AmazonRoute5.3 RecoveryControl ConfigFull 액세스 AmazonRoute53 RecoveryControl ConfigRead OnlyAccess	2021년 8월 18일
Route 53 ARC 변경 내용 추적 시작	Route 53 ARC는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 7월 27일

Amazon Route 53 Application Recovery Controller 자격 증명 및 액세스 문제 해결

다음 정보를 사용하면 Amazon Route 53 애플리케이션 복구 컨트롤러 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

주제

- Route 53 ARC에서 작업을 수행할 권한이 없음
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 Route 53 ARC AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

Route 53 ARC에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 route53-recovery-readiness:*GetWidget* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 route53-recovery-readiness:GetWidget on resource: my-example-widget
```

이 경우 Mateo는 *my-example-widget* 작업을 사용하여 route53-recovery-readiness:*GetWidget* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Route 53 ARC에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 AWS 서비스 수 있는 기능도 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 Route 53 ARC에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 Route 53 ARC AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제

어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Route 53 ARC에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon Route 53 애플리케이션 복구 컨트롤러 기능이 IAM과 함께 작동하는 방식 섹션을 참조하세요.
- 소유한 리소스에 대한 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오. AWS 계정
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

Amazon Route 53 Application Recovery Controller의 로깅 및 모니터링

모니터링은 Amazon Route 53 애플리케이션 복구 컨트롤러와 AWS 솔루션의 가용성과 성능을 유지하는 데 있어 중요한 부분입니다. 다중 지점 장애가 발생할 경우 이를 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집해야 합니다. AWS Route 53 ARC 리소스 및 활동을 모니터링하고 잠재적 사고에 대응하기 위한 여러 도구를 제공합니다 (예: Amazon) CloudWatch. AWS CloudTrail

Route 53 ARC의 각 기능에 대한 모니터링에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 영역 이동에 대한 로깅 및 모니터링
- 구역 자동 변속 로깅 및 모니터링
- 라우팅 제어를 위한 로깅 및 모니터링
- 준비 상태 확인을 위한 로깅 및 모니터링

Amazon Route 53 Application Recovery Controller의 규정 준수 검증

타사 감사자는 여러 규정 준수 프로그램의 일환으로 Amazon Route 53 애플리케이션 복구 컨트롤러의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램별 범위 내 규정 준수 프로그램AWS 서비스 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에

대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.

- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Amazon Route 53 Application Recovery Controller의 복원성

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다 AWS 리전 . AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

Route 53 ARC는 AWS 글로벌 인프라 외에도 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 제공합니다.

Amazon Route 53 Application Recovery Controller의 인프라 보안

Amazon Route 53 애플리케이션 복구 컨트롤러는 관리형 서비스로서 AWS 글로벌 네트워크 보안의 보호를 받습니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Route 53 ARC에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

Amazon Route 53 Application Recovery Controller 개발자 안내서에 대한 문서 기록

다음 항목은 Amazon Route 53 Application Recovery Controller 설명서의 중요한 변경 사항을 설명합니다.

- 버전: 최신
- 최신 설명서 업데이트: 2024년 4월 30일

변경 사항	설명	날짜
각 역량에 따른 문서 재구성	개발자 가이드 콘텐츠를 재구성하여 하위 개발 가이드로 격리합니다. 즉, 이제 Route 53 ARC의 각 기능에 대한 포괄적인 정보 (다중 AZ 복구를 위한 영역 이동 및 영역 자동 이동, 다중 지역 복구를 위한 라우팅 제어 및 준비 확인) 를 포함하는 별도의 섹션이 있습니다. 자세한 내용은 Amazon Route 53 애플리케이션 복구 컨트롤러란 무엇입니까? 를 참조하십시오.	2024년 4월 30일
영역 자동 전환 기능 추가	Route 53 ARC에 사용자 대신 가용 영역에서 애플리케이션의 리소스 트래픽을 이동할 수 있는 권한을 AWS 부여하여 이벤트 중 복구 시간을 줄이는 데 도움이 되는 새로운 기능을 추가합니다. 자세한 내용은 Amazon Route 53 Application Recovery	2023년 11월 30일

변경 사항	설명	날짜
	Controller의 영역 자동 전환을 참조하세요.	
새 서비스 연결 역할 추가	영역 자동 전환 연습 실행을 위한 새로운 서비스 연결 역할을 추가합니다. AWSServiceRoleForZonalAutoshiftPracticeRun 자세한 내용은 서비스 연결 역할 권한을 참조하십시오. AWSServiceRoleForZonalAutoshiftPracticeRun	2023년 11월 30일
클러스터에 크로스 계정 지원 추가	Route 53 ARC에서 클러스터에 대한 교차 계정 지원을 추가하여 하나의 클러스터를 사용하여 여러 AWS 계정이 소유한 제어판과 라우팅 제어를 쉽고 안전하게 호스팅할 수 있습니다. AWS Resource Access Manager 자세한 내용은 Route 53 ARC의 클러스터 크로스 계정 지원을 참조하세요.	2023년 10월 18일

변경 사항	설명	날짜
관리형 정책 업데이트	공유 AWS Resource Access Manager 리소스의 리소스 정책에 대한 세부 정보 반환을 지원하기 위해 `GetResourcePolicy` 권한을 추가하도록 `AmazonRoute53RecoveryControlConfigReadOnly` 관리형 정책을 업데이트합니다. 자세한 내용은 AWS 관리형 정책 단원을 참조하세요.	2023년 9월 19일
서비스 연결 역할 업데이트	Amazon EC2 인스턴스 폴링을 지원하기 위해 Route 53 ARC의 서비스 연결 역할에 새 권한 `ec2:DescribeVpnGateways` 및 `ec2:DescribeCustomerGateways` 를 추가했습니다. 자세한 내용은 Route 53 ARC에 서비스 연결 역할 사용을 참조하세요.	2023년 2월 17일
영역 전환을 위한 GA 릴리스	Route 53 ARC에 대한 영역 전환의 GA 릴리스를 지원합니다. 여기에는 영역 전환을 위해 Route 53 ARC에 등록된 관리형 리소스에 대한 ABAC(속성 기반 액세스 제어)가 포함됩니다. 자세한 내용은 Route 53 ARC과 함께하는 ABAC(속성 기반 액세스 제어)를 참조하세요.	2023년 1월 10일

변경 사항	설명	날짜
새로운 다중 AZ 영역 전환 추가	다중 AZ 애플리케이션을 위한 Route 53 ARC의 새로운 서비스인 영역 전환을 설명하는 콘텐츠가 추가되었습니다. 영역 전환을 시작하여 로드 밸런서 리소스에 대한 트래픽을 가용 영역에서 일시적으로 이동할 수 있습니다. 자세한 내용은 Route 53 ARC의 영역 전환을 참조하세요.	2022년 11월 28일
서비스 연결 역할 업데이트	Route 53 ARC의 서비스 연결 역할에 Lambda 함수에 대한 정보를 쿼리할 수 있는 새 권한 `lambda:ListProvisionedConcurrencyConfigs` 를 추가했습니다. 자세한 내용은 Route 53 ARC에 서비스 연결 역할 사용을 참조하세요.	2022년 8월 31일
관리형 정책이 업데이트됨	Amazon Route 53 권한을 제거하고 이를 선택 사항으로 나열하도록 `AmazonRoute53RecoveryControlConfigFullAccess` 관리형 정책을 업데이트했습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller의AWS 관리형 정책을 참조하세요.	2022년 5월 26일

변경 사항	설명	날짜
관리형 정책이 업데이트됨	필수 Amazon Route 53 권한을 포함하도록 `AmazonRoute53RecoveryControlConfigFullAccess` 관리형 정책을 업데이트했습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller의AWS 관리형 정책을 참조하세요.	2022년 4월 15일
새 목록 라우팅 제어 API에 대한 CLI 예제 추가	매우 안정적인 Route 53 ARC 데이터 영역 API에 포함된 새로운 목록 라우팅 제어 API 작업에 대한 예제 CLI 명령 및 모범 사례 권장 사항을 추가했습니다. 자세한 내용은 라우팅 제어와 상태 나열 및 업데이트를 참조하세요.	2022년 3월 31일
안전 규칙 재정의에 대한 지원 추가	안전 규칙 재정의에 대한 지원이 추가되어 구성한 안전 규칙에 따라 적용되는 라우팅 제어 보호를 우회할 수 있습니다. 예를 들어 재해 복구를 위한 장애 조치 중에 “break glass” 시나리오에서 안전 규칙 재정의가 필요할 수 있습니다. 자세한 내용은 안전 규칙을 재정의하여 트래픽 다시 라우팅을 참조하세요.	2022년 3월 2일

변경 사항	설명	날짜
추가 태깅 지원 추가	Route 53 ARC에서 클러스터, 제어판, 라우팅 제어, 안전 규칙 등 추가 리소스에 태그를 지정하는 지원이 추가되었습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller에서 태그 지정을 참조하세요.	2021년 12월 20일
관리형 정책이 업데이트됨	리소스에 대한 태그를 나열할 수 있는 권한을 추가한 `AmazonRoute53RecoveryControlConfigReadOnly` 관리형 정책을 업데이트했습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller의AWS 관리형 정책을 참조하세요.	2021년 12월 20일
실시간 알림 지원을 다음과 같이 추가했습니다. EventBridge	에 대한 지원이 추가되었습니다. 즉 EventBridge, 상태가 READY에서 NOT READY로 변경될 때와 같이 이제 알림을 받고 Route 53 ARC 준비 상태 검사 상태 변경 시 조치를 취하는 규칙을 추가할 수 있습니다. 자세한 내용은 Amazon에서 Route 53 ARC 사용을 참조하십시오 EventBridge.	2021년 12월 20일

변경 사항	설명	날짜
라우팅 제어 상태 코드 샘플 추가	API 작업을 사용하여 라우팅 제어 상태를 가져오거나 업데이트할 때 클러스터 엔드포인트를 순서대로 시도하는 방법을 보여주는 코드 샘플이 추가되었습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller의 API 예제를 참조하세요.	2021년 11월 16일
읽기 전용 정책에 새로운 권한 추가	정책 `AmazonRoute53RecoveryReadinessReadOnlyAccess` 에 두 개의 새로운 권한 `route53-recovery-readiness:GetArchitectureRecommendations` 및 `route53-recovery-readiness:GetCellReadinessSummary` 를 추가했습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller의AWS 관리형 정책을 참조하세요.	2021년 11월 9일

변경 사항	설명	날짜
Amazon API Gateway 리소스 유형에 대한 지원 추가	새 리소스 유형인 Amazon API Gateway를 추가하고, Route 53 ARC가 준비 상태 확인을 통해 API Gateway를 감사할 수 있도록 Route 53 ARC 서비스 연결 역할 권한을 업데이트했습니다. 자세한 내용은 준비 규칙 및 지원되는 리소스 유형 및 Route 53 ARC의 서비스 연결 역할 사용을 참조하세요.	2021년 10월 28일
Lambda 함수 리소스 유형에 대한 지원 추가	새 리소스 유형인 Lambda 함수를 추가하고, Route 53 ARC가 준비 상태 확인을 통해 Lambda 함수를 감사할 수 있도록 Route 53 ARC 서비스 연결 역할 권한을 업데이트했습니다. 자세한 내용은 준비 규칙 및 지원되는 리소스 유형 및 Route 53 ARC의 서비스 연결 역할 사용을 참조하세요.	2021년 10월 8일
CloudFormation 및 Terraform 템플릿에 대한 링크 추가	Route 53 Arc 사용을 빠르게 시작할 수 있도록 다운로드 가능한 AWS CloudFormation Hashicorp Terraform 템플릿에 대한 링크를 추가했습니다. 자세한 내용은 새 애플리케이션을 통한 복구 준비를 참조하십시오.	2021년 9월 13일

변경 사항	설명	날짜
새로운 관리형 정책 추가	Route 53 ARC에 다음과 같은 AWS 관리형 정책을 추가했습니다: `AmazonRoute53RecoveryReadinessFullAccess` `AmazonRoute53RecoveryReadinessReadOnlyAccess` `AmazonRoute53RecoveryClusterFullAccess` ,`AmazonRoute53RecoveryClusterReadOnlyAccess` ,`AmazonRoute53RecoveryControlConfigFullAccess` , 및`AmazonRoute53RecoveryControlConfigReadOnlyAccess` . 자세한 내용은 Amazon Route 53 Application Recovery Controller의AWS 관리형 정책을 참조하세요.	2021년 8월 18일
Amazon Route 53 애플리케이션 복구 컨트롤러에 대한 AWS 관리형 정책 추적 시작	관리형 정책에 대한 업데이트는 초기 릴리스 날짜부터 추적됩니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller의AWS 관리형 정책을 참조하세요.	2021년 7월 27일

변경 사항	설명	날짜
Amazon Route 53 Application Recovery Controller의 첫 번째 릴리스	Route 53 ARC는 한 지역 내에서 또는 여러 AWS 지역에 걸쳐 페일오버를 중앙에서 조정하여 애플리케이션 가용성을 개선합니다. Route 53 ARC는 애플리케이션이 장애 조치 트래픽을 처리하도록 확장되고 장애를 우회하여 라우팅되도록 구성되었는지 확인하기 위해 준비 확인을 제공합니다. 또한 매우 안정적인 라우팅 제어를 제공하므로 가용 영역 또는 리전 간에 트래픽을 다시 라우팅하여 애플리케이션을 복구할 수 있습니다. 자세한 내용은 Route 53 ARC란 무엇입니까?를 참조하세요.	2021년 7월 27일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.