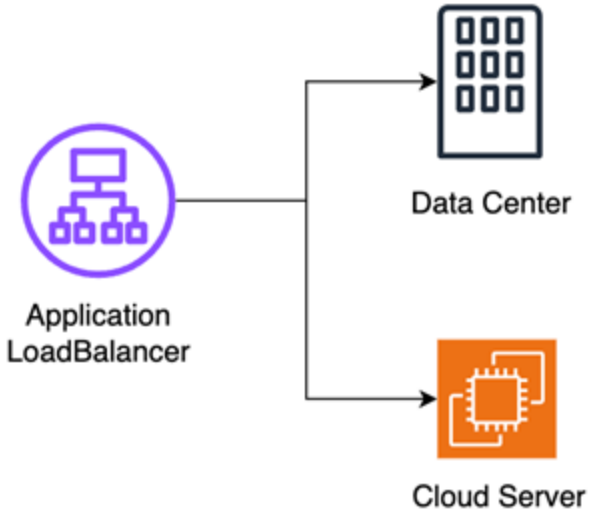
ALB를 활용한 하이브리드 클라우드

자동 장애 전환 구조 설계 경험 공유

장수정

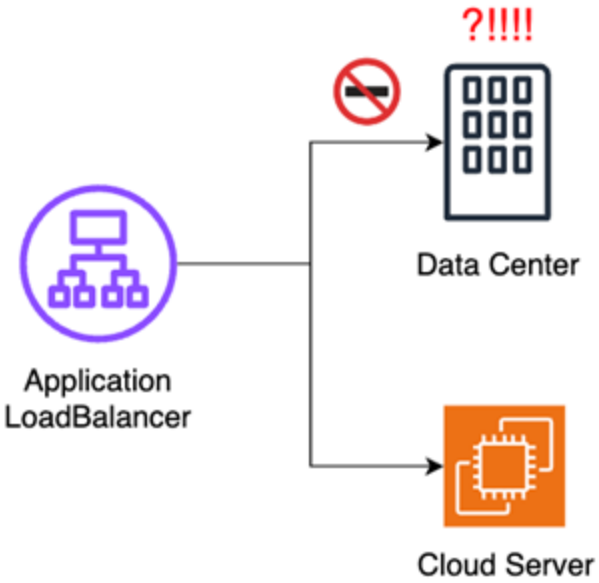
E-mail : diverserjang@gmail.com
LinkedIn : sjjang97

인프라 구조



✓ 사용자의 요청은 먼저 AWS에 도달한 뒤, ALB에서 트래픽을 Cloud와 IDC로 일정 비율로 분산 처리하도록 구성되어 있음.

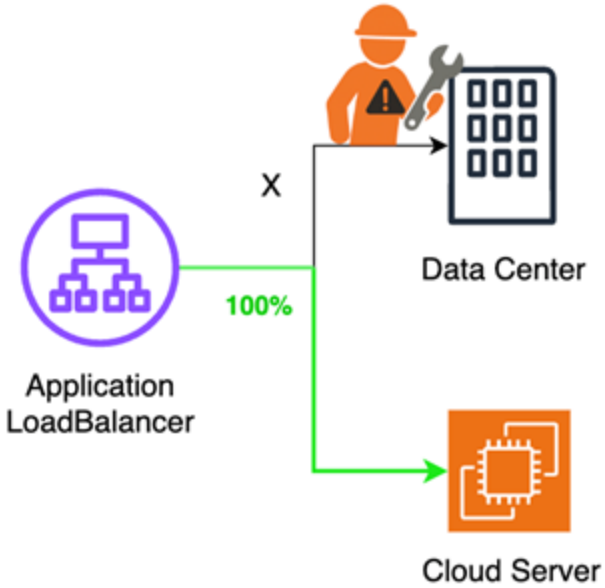
이슈 발생



✓ IDC 통신장비에 장애가 발생하여 IDC 쪽으로 흘러가던 트래픽이 모두 TimeOut 에러가 발생했음.

✓ 일부 사용자는 응답 지연 또는 서비스가 끊기는 경험을 하게됨.

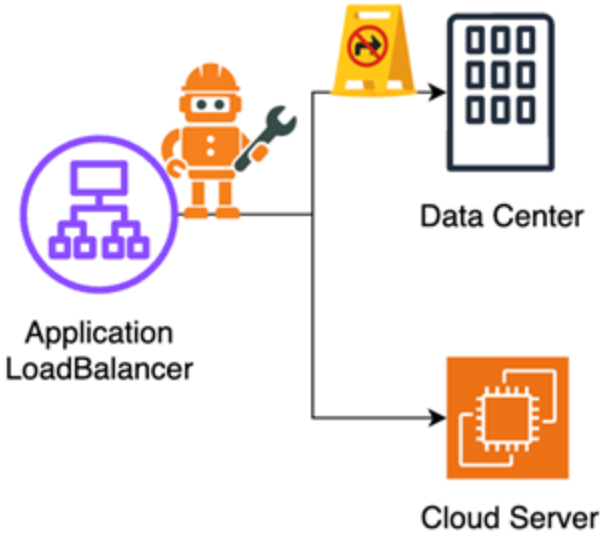
이슈 대응



✓ ALB의 가중치 기반 분기 구조는, 한쪽 대상에 장애가 나도 자동으로 우회되지 않음.

✓ 이에 IDC 장비를 복구하는 동안, 트래픽 처리를 위해 Cloud 쪽으로 트래픽을 수동 전환함.

기존 트래픽 전환 구조의 한계 및 신규 프로세스 도입 필요성

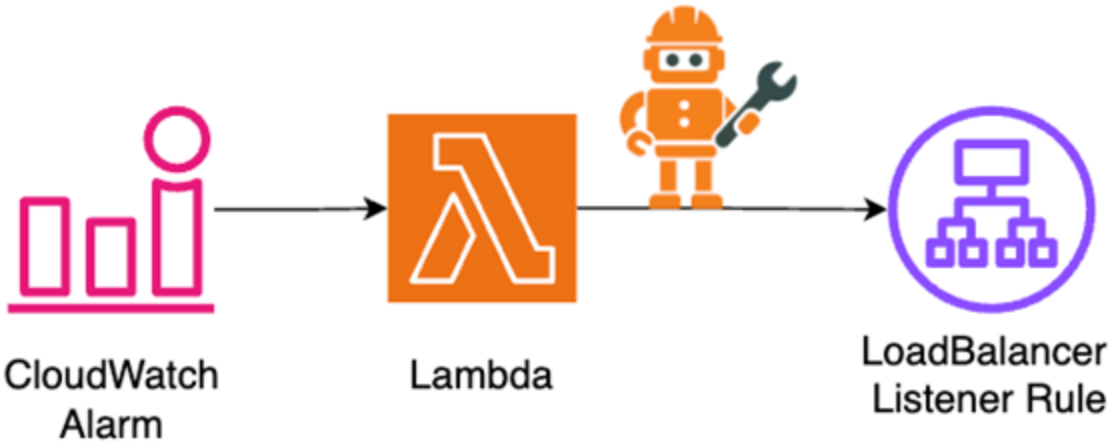


✓ 한계

1. 수동으로 여러 AWS 계정에 접속하여 ALB 리스너 규칙을 직접 수정해야함.
2. 야간, 무인 시간대 대응이 늦어질 수 있음.

→ 수동 개입 없이 야간, 무인 시간에도 대응 가능하도록 자동 전환 구조 도입하기로 함.

자동 전환 구조 동작 흐름



✓ 지표 기반으로 자동 감시할 수 있도록 CloudWatch 알람을 설정함.

✓ 알람이 울리면, 서버리스로 코드를 실행할 수 있는 Lambda가 실행됨.

✓ Lambda가 여러 계정에 있는 ALB 리스너 규칙을 변경함.

지표 기반 복합 경보 설정

1. HealthyHostCount 지표 기반 단일경보 생성
   : 정상 상태로 간주되는 대상 수
2. TargetConnectionErrorCount 지표 기반 단일경보 생성
   : 로드 밸런서와 대상 사이에 성공적으로 구성되지 않은 연결 수

1번 경보발생 AND 2번 경보발생 일 때 복합경보가 경보상태로 전환됨.

→ 위 복합경보 발생 시 Lambda를 실행함.

Lambda 실행흐름 / 작동 요구사항

1. 복합 경보로 실행된 것인지 확인
2. 환경변수에 등록된 대상 ALB Rule ARN / Listener ARN에 따라 ALB 리스너 규칙 또는 기본 동작을 수정함.
3. 동일 계정은 바로 실행, 다른 계정은 STS AssumRule을 통해 권한 위임 후 수정

필요 권한

```
"Action": [
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:ModifyRule",
    "elasticloadbalancing:ModifyListener"
],
```

Lambda가 프라이빗 통신을 하는경우

- Elasticloadbalancing Endpoint
- STS Endpoint

VPC Endpoint 필요 이유

Lambda 코드에서 호출하는 API

1. modify_rule() : ALB의 특정 리스너 규칙(Rule)의 Action, Weight을 수정하는 API
2. modify_listener() : ALB 리스너의 속성을 변경하는 API 입니다. 해당 코드에서는 리스너의 Default Action을 수정
3. sts client의 assume_role() : 다른 AWS 계정 또는 동일 계정 내에서 특정 IAM Role을 임시로 가정하는 API

→ ElasticLoadbalancing v2 서비스, STS 서비스와 통신이 필요함.

이에 Elasticloadbalancing Endpoint, STS Endpoint를 생성한 것임.

추가 고려사항 : 알람 설정

발생 가능 예외	원인	비고
AccessDeniedException	IAM 권한 부족 (ELB, STS API 호출 시)	Role이 올바르게 설정되지 않았거나, Assume Role 권한이 없음
ResourceNotFoundException	ALB Rule 또는 Target Group이 삭제됨	사용 중인 RuleArn 또는 TargetGroupArn이 삭제된 경우
NetworkingError	VPC Endpoint 미설정 또는 AWS API 접속 불가	VPC 내부에서 PrivateLink 미설정 시 발생 가능

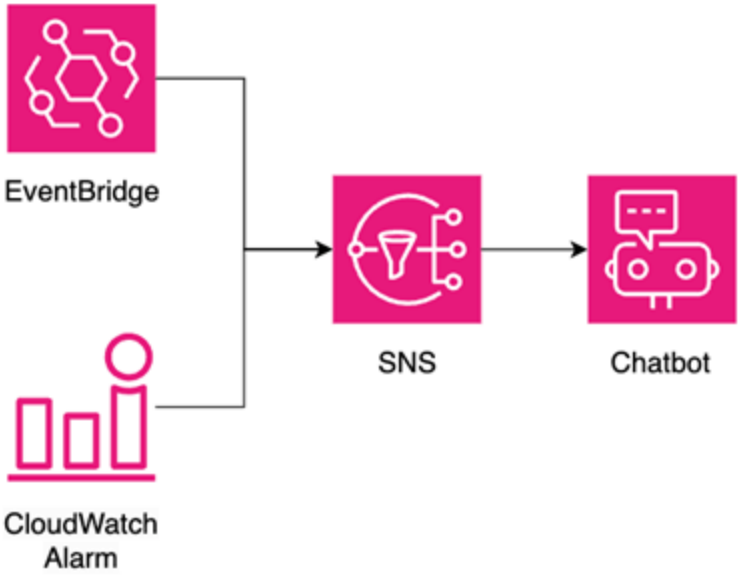
→ 규칙이나 리소스 변경을 바로 감지할 수 있는 체계를 구성

중요 리소스 변경 이벤트 감지 및 알림 구성

1. 특정 Role에 수정/삭제가 일어난 경우 (DeleteRole/UpdateRole/DeleteRolePolicy)
2. LoadBalancer에 변경/삭제가 일어난 경우
   (SetRulePriorities/ModifyRule/DeleteRule)
3. VPC Endpoint 수정/삭제가 일어난 경우 (DeleteVpcEndpoints/ModifyVpcEndpoint)
4. Lambda 함수 관련 이벤트 발생의 경우
   (UpdateFunctionCode/UpdateFunctionConfiguration/DeleteFunction
   Success rate (%) / AWS/Lambda Errors)
5. 단일, 복합경보 변경/삭제가 일어난 경우 (update/delete)

→ 위 이벤트 발생시 Slack 으로 알림 전송됨.

중요 리소스 변경 이벤트 감지 및 알림 구성



느낀점

✓ 작은 설정 하나가 전체 동작을 무너뜨릴 수 있다.

✓ 인프라는 디테일 하나에 좌우된다.

감사합니다.