구현 안내서

# AWS에서 워크로드 검색

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS에서 워크로드 검색: 구현 안내서

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon 계열사, 관련 업체 또는 Amazon의 지원 업체 여부에 상관없이 해당 소유자의 자산입니다.

# Table of Contents

솔루션 개요 ..... 1
기능 및 이점 ..... 2
사용 사례 ..... 3
개념 및 정의 ..... 3
아키텍처 개요 ..... 5
아키텍처 다이어그램 ..... 5
AWS Well-Architected 설계 고려 사항 ..... 7
운영 우수성 ..... 7
보안 ..... 7
신뢰성 ..... 8
성능 효율성 ..... 8
비용 최적화 ..... 8
지속 가능성 ..... 9
아키텍처 세부 정보 ..... 10
인증 메커니즘 ..... 10
지원되는 리소스 ..... 10
AWS 아키텍처 다이어그램 관리의 워크로드 검색 ..... 10
웹 UI 및 스토리지 관리 ..... 10
데이터 구성 요소 ..... 11
이미지 배포 구성 요소 ..... 13
검색 구성 요소 ..... 13
비용 구성 요소 ..... 14
이 솔루션의 AWS 서비스 ..... 15
배포 계획 ..... 18
지원되는 AWS 리전 ..... 18
비용 ..... 19
비용 테이블 예 ..... 19
보안 ..... 21
리소스 액세스 ..... 21
네트워크 액세스 ..... 21
애플리케이션 구성 ..... 22
할당량 ..... 23
이 솔루션의 AWS 서비스 할당량 ..... 23
AWS CloudFormation 할당량 ..... 23

AWS Lambda 할당량 ... 23
Amazon VPC 할당량 ... 24
배포 계정 선택 ... 24
솔루션 배포 ... 25
배포 프로세스 개요 ... 25
사전 조건 ... 25
배포 파라미터 세부 정보 수집 ... 25
AWS CloudFormation 템플릿 ... 28
스택 시작 ... 28
배포 후 구성 작업 ... 36
Amazon Cognito에서 고급 보안 켜기 ... 36
Amazon Cognito 사용자 생성 ... 36
추가 사용자를 생성하려면: ... 36
AWS에서 워크로드 검색에 로그인 ... 38
리전 가져오기 ... 38
리전 가져오기 ... 39
AWS CloudFormation 템플릿 배포 ... 40
CloudFormation StackSets를 사용하여 계정 간에 글로벌 리소스 프로비저닝 ... 40
CloudFormation StackSets를 사용하여 리전 리소스 프로비저닝 ... 41
CloudFormation을 사용하여 스택을 배포하여 글로벌 리소스 프로비저닝 ... 43
CloudFormation을 사용하여 스택을 배포하여 리전 리소스 프로비저닝 ... 44
리전을 올바르게 가져왔는지 확인 ... 45
비용 기능 설정 ... 45
배포 계정에서 AWS 비용 및 사용 보고서 생성 ... 45
외부 계정에서 AWS 비용 및 사용 보고서 생성 ... 46
복제 설정 ... 48
S3 버킷 수명 주기 정책 편집 ... 49
솔루션 모니터링 ... 50
myApplications ... 50
CloudWatch AppInsights ... 50
솔루션 업데이트 ... 51
문제 해결 ... 52
알려진 문제 해결 ... 52
Config 전송 채널 오류 ... 52
기존 VPC에 배포할 때 Resolver 스택 배포 시간 초과 검색 ... 52
계정을 가져온 후 검색되지 않은 리소스 ... 53

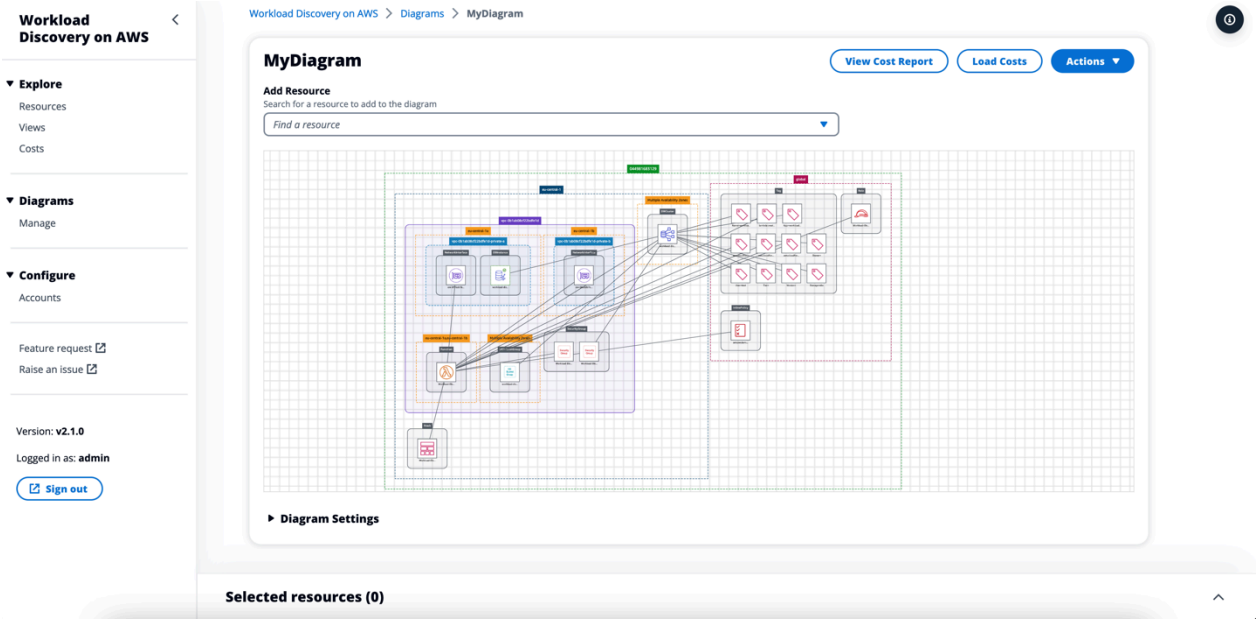
특정 계정에서 AWS가 아닌 AWS Config 리소스만 검색되고 있습니다. ..... 54
AWS Support에 문의 ..... 55
사례 생성 ..... 55
어떻게 도와드릴까요? ..... 55
추가 정보 ..... 55
사례를 더 빠르게 해결할 수 있도록 지원 ..... 55
지금 해결하거나 문의하기 ..... 55
솔루션 제거 ..... 57
AWS 관리 콘솔 사용 ..... 57
AWS 명령줄 인터페이스 사용 ..... 57
개발자 안내서 ..... 58
소스 코드 ..... 58
배포 리소스 찾기 ..... 58
지원되는 리소스 ..... 58
AWS Organizations 계정 검색 모드 ..... 59
Amazon S3 복제 역할 작업 ..... 60
S3 버킷 정책 ..... 61
AWS API ..... 62
API Gateway ..... 62
Cognito ..... 62
구성 ..... 63
DynamoDB Streams ..... 63
Amazon EC2 ..... 63
Amazon Elastic Load Balancer ..... 63
Amazon Elastic Kubernetes 서비스 ..... 63
IAM ..... 63
Lambda ..... 64
OpenSearch Service ..... 64
Organizations ..... 64
Amazon Simple Notification Service ..... 64
Amazon Security Token Service ..... 64
레퍼런스 ..... 65
익명화된 데이터 수집 ..... 65
기여자 ..... 66
개정 ..... 67
고지 사항 ..... 68

..... lxix

# AWS 클라우드 워크로드의 아키텍처 다이어그램을 자동으로 생성하는 시각화 도구 배포

Amazon Web Services(AWS) 클라우드 워크로드 모니터링은 운영 상태 및 효율성을 유지하는 데 매우 중요합니다. 그러나 AWS 리소스와 리소스 간의 관계를 추적하는 것은 어려울 수 있습니다. AWS의 워크로드 검색은 AWS의 워크로드에 대한 아키텍처 다이어그램을 자동으로 생성하는 시각화 도구입니다. 이 솔루션을 사용하여 AWS의 라이브 데이터를 기반으로 세부 워크로드 시각화를 빌드, 사용자 지정 및 공유할 수 있습니다.

이 솔루션은 계정 및 리전 전체에서 AWS 리소스의 인벤토리를 유지하고, 리소스 간의 관계를 매핑하고, 웹 사용자 인터페이스(웹 UI)에 표시하는 방식으로 작동합니다. 리소스를 변경할 때 AWS의 워크로드 검색은 AWS 관리 콘솔의 리소스에 대한 링크를 제공하여 시간을 절약합니다.




AWS의 워크로드 검색에서 생성된 샘플 아키텍처 다이어그램

이 구현 가이드에서는 AWS 클라우드에서 AWS에 워크로드 검색을 배포하기 위한 아키텍처 고려 사항 및 구성 단계를 설명합니다. 여기에는 보안 및 가용성에 대한 AWS 모범 사례를 사용하여이 솔루션을 배포하는 데 필요한 AWS 서비스를 시작하고 구성하는 AWS CloudFormation 템플릿에 대한 링크가 포함되어 있습니다.

환경에서 AWS에서 워크로드 검색을 구현하려는 대상에는 솔루션 아키텍트, 비즈니스 의사 결정자, DevOps 엔지니어, 데이터 과학자 및 클라우드 전문가가 포함됩니다.

이 탐색 테이블을 사용하여 다음 질문에 대한 답을 빠르게 찾을 수 있습니다.

| 다음을 수행하려는 경우 . . . | 읽기 . . . |
| --- | --- |
| 이 솔루션을 실행하는 데 드는 비용을 파악합니다.<br><br>미국 동부(버지니아 북부) 리전에서이 솔루션을 실행하는 데 드는 예상 비용은 매월 USD $425.19입니다. | 비용 |
| 이 솔루션의 보안 고려 사항을 이해합니다. | 보안 |
| 이 솔루션의 할당량을 계획하는 방법을 파악합니다. | 할당량 |
| 이 솔루션을 지원하는 AWS 리전을 파악합니다. | 지원되는 AWS 리전 |
| 이 솔루션에 포함된 AWS CloudFormation 템플릿을 보거나 다운로드하여이 솔루션의 인프라 리소스("스택")를 자동으로 배포합니다. | AWS CloudFormation 템플릿 |
| 소스 코드에 액세스합니다. | GitHub 리포지토리 |

# 기능 및 이점

AWS의 워크로드 검색은 다음과 같은 기능을 제공합니다.

실시간에 가까운 데이터를 사용하여 아키텍처 다이어그램 구축

AWS의 워크로드 검색은 15분마다 계정을 스캔하여 생성한 다이어그램이 워크로드를 정확하고 최신으로 표현하고 있는지 확인합니다.

한 곳에서 여러 계정 및 리전의 리소스 보기

이 솔루션은 중앙 집중식 그래프 데이터베이스에서 AWS 계정 및 리전 전반의 AWS 리소스 인벤토리를 유지 관리하므로 단일 UI에서 여러 계정 및 리전과 서로의 관계를 탐색할 수 있습니다.

AWS Organizations 통합

AWS Organizations를 사용하여 솔루션을 배포할 때 AWS의 워크로드 검색은 조직에서 지원되는 모든 리소스를 자동으로 검색합니다. 이 구성에서는 계정별 CloudFormation 템플릿의 배포를 직접 관리하여 이러한 계정을 검색할 수 있도록 할 필요가 없습니다.

워크로드 간 비용 데이터 수집

활성화하면 비용 기능을 사용하여 계정의 리소스를 비용별로 검색하고 찾은 리소스를 다이어그램에 추가할 수 있습니다. 기존 다이어그램에 비용 데이터를 추가할 수도 있습니다.

diagrams.net://(이전 draw.io://)로 내보내기

AWS의 워크로드 검색은 다이어그램을 내보낼 수 있으므로이 타사 그리기 소프트웨어를 사용하여 다이어그램에 주석을 더 달 수 있습니다.

AWS Systems Manager의 기능인 AWS Service Catalog AppRegistry AWS Systems Manager와 통합

이 솔루션에는 솔루션의 CloudFormation 템플릿과 기본 리소스를 Service Catalog AppRegistry 및 Application Manager 모두에서 애플리케이션으로 등록하는 Service Catalog AppRegistry 리소스가 포함되어 있습니다. 이 통합을 통해 솔루션의 리소스를 중앙에서 관리하고 애플리케이션 검색, 보고 및 관리 작업을 활성화할 수 있습니다.

# 사용 사례

설계 및 보안 검토

이 솔루션을 사용하여 아키텍처 다이어그램을 생성하여 워크로드 구현이 제안된 설계와 일치하는지 검증합니다.

기존 워크로드 탐색 및 문서화

아키텍처 다이어그램을 생성하여 설명서가 거의 없거나 코드형 인프라 없이 수동으로 배포된 워크로드를 탐색합니다.

비용 시각화

예상 비용에 대한 개요가 포함된 아키텍처 다이어그램에 대한 비용 보고서를 생성합니다.

# 개념 및 정의

이 섹션에서는 이 솔루션과 관련된 핵심 개념 및 용어에 대해 설명합니다.

리소스

Amazon Simple Storage Service(Amazon S3) 버킷 또는 AWS AWS Lambda 리소스입니다.

관계

AWS Identity and Access Management(IAM) 역할과 연결된 AWS Lambda 함수와 같은 두 리소스 간의 링크입니다.

리소스 유형

리소스의 분류 범주입니다. 항상와 같은 CloudFormation 명명 규칙을 따릅니다`AWS::Lambda::Function`.

discovery

솔루션이 AWS 계정 및 리전에서 리소스와 해당 관계를 매핑하기 위해 시작하는 프로세스입니다.

계정 검색 모드

계정을 검색하고 솔루션에 추가하는 방법으로, AWS UI에서 워크로드 검색을 통해 자체 관리되거나 AWS Organizations에 위임됩니다.

> **Note**
>
> AWS 용어에 대한 일반적인 참조는 AWS 용어집을 참조하십시오.

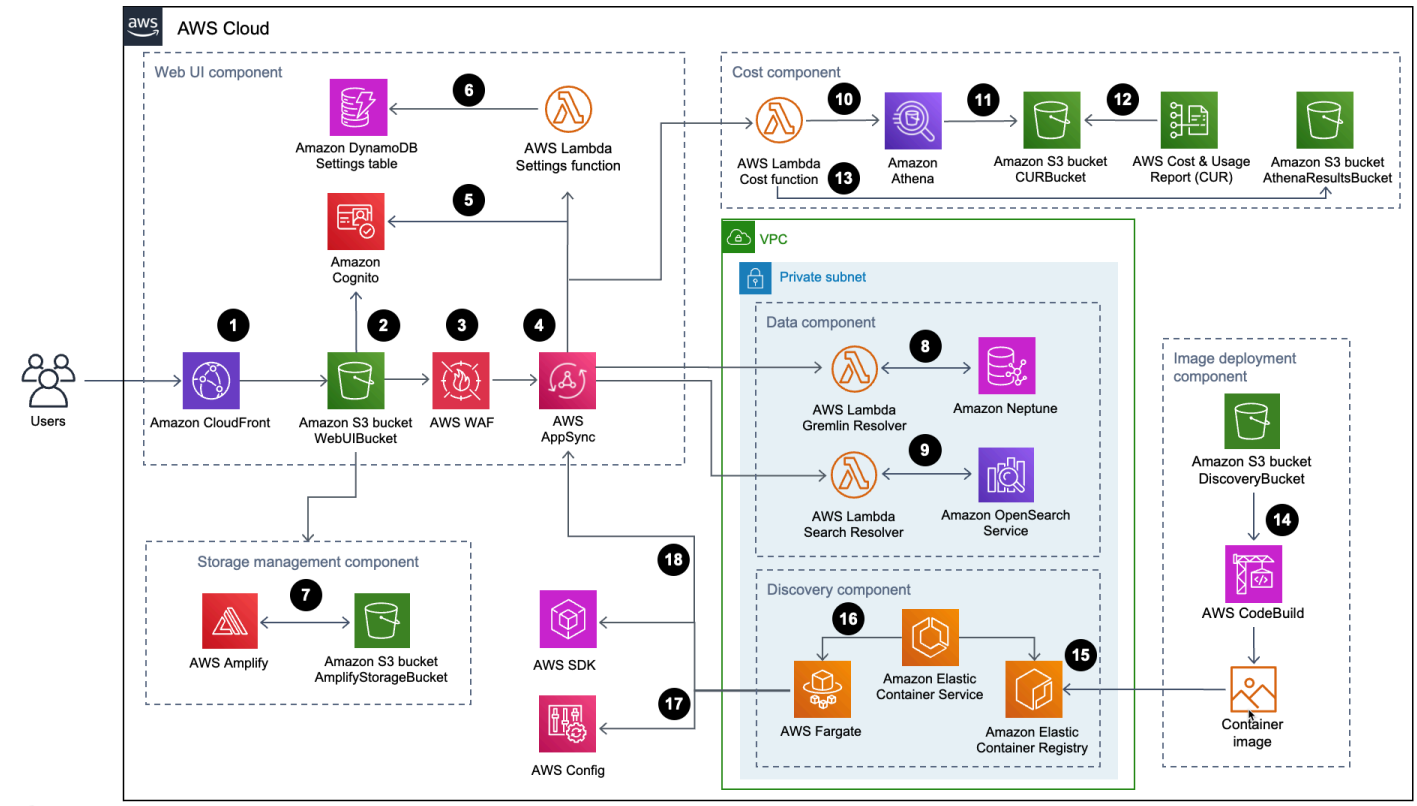
# 아키텍처 개요

이 섹션에서는 이 솔루션과 함께 배포된 구성 요소에 대한 참조 구현 아키텍처 다이어그램을 제공합니다.

## 아키텍처 다이어그램

이 솔루션을 기본 파라미터와 함께 배포하면 AWS 클라우드에서 다음 환경이 빌드됩니다.

AWS 아키텍처의 워크로드 검색




AWS CloudFormation 템플릿과 함께 배포된 솔루션 구성 요소의 상위 수준 프로세스 흐름은 다음과 같습니다.

1. HTTP Strict-Transport-Security(HSTS)는 Amazon CloudFront 배포의 각 응답에 보안 헤더를 추가합니다.
2. Amazon Simple Storage Service(Amazon S3) 버킷은 Amazon CloudFront와 함께 배포되는 웹 UI를 호스팅합니다. Amazon Cognito는 웹 UI에 대한 사용자 액세스를 인증합니다.

3. AWS WAF는 가용성에 영향을 미치거나, 보안을 손상시키거나, 과도한 리소스를 소비할 수 있는 일반적인 악용 및 봇으로부터 AppSync API를 보호합니다.
4. AWS AppSync 엔드포인트를 사용하면 웹 UI 구성 요소가 리소스 관계 데이터를 요청하고, 비용을 쿼리하고, 새 AWS 리전을 가져오고, 기본 설정을 업데이트할 수 있습니다. 또한 AWS AppSync를 사용하면 검색 구성 요소가 솔루션의 데이터베이스에 영구 데이터를 저장할 수 있습니다.
5. AWS AppSync는 Amazon Cognito에서 프로비저닝한 JSON 웹 토큰(JWTs)을 사용하여 각 요청을 인증합니다.
6. `Settings` AWS Lambda 함수는 가져온 리전 및 기타 구성을 Amazon DynamoDB에 유지합니다.
7. 이 솔루션은 AWS Amplify와 Amazon S3 버킷을 스토리지 관리 구성 요소로 배포하여 사용자 기본 설정과 저장된 아키텍처 다이어그램을 저장합니다.
8. 데이터 구성 요소는 `Gremlin Resolver` AWS Lambda 함수를 사용하여 Amazon Neptune 데이터베이스에서 데이터를 쿼리하고 반환합니다.
9. 데이터 구성 요소는 `Search Resolver` Lambda 함수를 사용하여 리소스 데이터를 쿼리하고 Amazon OpenSearch Service 도메인에 유지합니다.
10. `Cost` Lambda 함수는 Amazon Athena를 사용하여 AWS 비용 및 사용 보고서(AWS CUR)를 쿼리하여 예상 비용 데이터를 웹 UI에 제공합니다.
11. Amazon Athena는 AWS CUR에서 쿼리를 실행합니다.
12. AWS CUR은 `CostAndUsageReportBucket` Amazon S3 버킷에 보고서를 전송합니다.
13. `Cost` Lambda 함수는 Amazon Athena 결과를 `AthenaResultsBucket` Amazon S3 버킷에 저장합니다.
14. AWS CodeBuild는 이미지 배포 구성 요소에 검색 구성 요소 컨테이너 이미지를 빌드합니다.
15. Amazon Elastic Container Registry(Amazon ECR)에는 이미지 배포 구성 요소에서 제공하는 도커 이미지가 포함되어 있습니다.
16. Amazon Elastic Container Service(Amazon ECS)는 AWS Fargate 작업을 관리하고 작업을 실행하는 데 필요한 구성을 제공합니다. AWS Fargate는 15분마다 컨테이너 작업을 실행하여 인벤토리 및 리소스 데이터를 새로 고칩니다.
17. AWS Config 및 AWS SDK 호출은 검색 구성 요소가 가져온 리전의 리소스 데이터 인벤토리를 유지한 다음 결과를 데이터 구성 요소에 저장하는 데 도움이 됩니다.
18. AWS Fargate 작업은 AppSync API에 대한 API 호출을 통해 Amazon Neptune 데이터베이스 및 Amazon OpenSearch Service 도메인에 대한 AWS Config 및 AWS SDK 호출의 결과를 유지합니다. OpenSearch

# AWS Well-Architected 설계 고려 사항

이 솔루션은 고객이 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적인 워크로드를 설계하고 운영할 수 있도록 지원하는 AWS Well-Architected Framework의 모범 사례를 사용합니다.

이 섹션에서는 Well-Architected Framework의 설계 원칙과 모범 사례가 이 솔루션에 어떤 이점을 제공하는지 설명합니다.

## 운영 우수성

이 솔루션을 활용하기 위해 운영 우수성 원칙의 원칙과 모범 사례를 사용하여이 솔루션을 설계했습니다.

- CloudFormation을 사용하여 코드형 인프라로 정의된 리소스입니다.
- 이 솔루션은 지표를 Amazon CloudWatch로 푸시하여 인프라, Lambda 함수, Amazon ECS 작업, AWS S3 버킷 및 나머지 솔루션 구성 요소에 대한 관찰성을 제공합니다.

## 보안

이 솔루션을 활용하기 위해 보안 원칙의 원칙과 모범 사례를 사용하여이 솔루션을 설계했습니다.

- Amazon Cognito는 웹 UI 앱 사용자를 인증하고 승인합니다.
- 솔루션에서 사용하는 모든 역할은 최소 권한 액세스를 따릅니다. 즉, 서비스가 제대로 작동하는 데 필요한 최소 권한만 포함됩니다.
- 저장 데이터 및 전송 데이터는 전용 키 관리 스토어인 AWS Key Management Service(AWS KMS)에 저장된 키를 사용하여 암호화됩니다.
- 자격 증명은 만료 기간이 짧으며 강력한 암호 정책을 따릅니다.
- AWS AppSync 보안 GraphQL 명령은 프런트엔드 및 백엔드에서 호출할 수 있는 작업을 세밀하게 제어할 수 있습니다.
- 해당하는 경우 로깅, 추적 및 버전 관리가 활성화됩니다.
- 해당하는 경우 자동 패치 적용(마이너 버전) 및 스냅샷 생성이 활성화됩니다.
- 네트워크 액세스는 기본적으로 프라이빗이며 Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트는 사용 가능한 경우 켜져 있습니다.

## 신뢰성

이 솔루션을 활용하기 위해 신뢰성 원칙의 원칙과 모범 사례를 사용하여이 솔루션을 설계했습니다.

- 이 솔루션은 가능한 경우 AWS 서버리스 서비스를 사용하여 서비스 장애로부터 고가용성과 복구를 보장합니다.
- 모든 컴퓨팅 처리는 Lambda 함수 또는 AWS Fargate의 Amazon ECS를 사용합니다.
- 모든 사용자 지정 코드는 AWS SDK를 사용하며 API 속도 할당량에 도달하지 않도록 클라이언트 측에서 요청이 제한됩니다.

## 성능 효율성

이 솔루션을 활용하기 위해 성능 효율성 원칙의 원칙과 모범 사례를 사용하여이 솔루션을 설계했습니다.

- 이 솔루션은 가능한 경우 AWS 서버리스 아키텍처를 사용합니다. 이렇게 하면 물리적 서버 관리의 운영 부담이 줄어듭니다.
- 이 솔루션은 AWS Lambda, Amazon Neptune, AWS AppSync, Amazon S3, Amazon Cognito와 같이이 솔루션에 사용되는 AWS 서비스를 지원하는 모든 리전에서 시작할 수 있습니다.
- 지원되는 리전에서 Amazon Neptune 서버리스를 사용하면 데이터베이스 용량을 관리하고 최적화할 필요 없이 그래프 워크로드를 실행하고 즉시 확장할 수 있습니다.
- 이 솔루션은 전체적으로 관리형 서비스를 사용하여 리소스 프로비저닝 및 관리의 운영 부담을 줄입니다.

## 비용 최적화

이 솔루션을 활용하기 위해 비용 최적화 원칙의 원칙과 모범 사례를 사용하여이 솔루션을 설계했습니다.

- AWS Fargate의 AWS ECS는 컴퓨팅에만 Lambda 함수를 사용하며 사용량에 따른 요금만 청구합니다.
- Amazon DynamoDB는 온디맨드로 용량을 확장하므로 사용하는 용량에 대해서만 비용을 지불하면 됩니다.

# 지속 가능성

이 솔루션을 활용하기 위해 지속 가능성 원칙의 원칙과 모범 사례를 사용하여이 솔루션을 설계했습니다.

- 이 솔루션은 가능한 경우 관리형 및 서버리스 서비스를 사용하여 백엔드 서비스의 환경 영향을 최소화합니다.

# 아키텍처 세부 정보

이 섹션에서는이 솔루션을 구성하는 구성 요소와 AWS 서비스와 이러한 구성 요소가 함께 작동하는 방식에 대한 아키텍처 세부 정보를 설명합니다.

## 인증 메커니즘

AWS의 워크로드 검색은 UI 및 AWS AppSync 인증 모두에 Amazon Cognito 사용자 풀을 사용합니다. 인증되면 Amazon Cognito는 모든 후속 API 요청과 함께 제공되는 JSON 웹 토큰(JWT)을 웹 UI에 제공합니다. 유효한 JWT가 제공되지 않으면 API 요청이 실패하고 HTTP 403 금지됨 응답을 반환합니다.

## 지원되는 리소스

AWS에서 워크로드 검색을 통해 계정 및 리전 내에서 검색할 수 있는 AWS 리소스 유형 목록은 지원되는 리소스를 참조하세요.

## AWS 아키텍처 다이어그램 관리의 워크로드 검색

CRUD(생성, 읽기, 업데이트 및 삭제) 작업을 수행할 수 있는 웹 UI를 사용하여 AWS 아키텍처 다이어그램에서 워크로드 검색을 저장할 수 있습니다. AWS Amplify 스토리지 API를 사용하면 AWS의 워크로드 검색을 통해 아키텍처 다이어그램을 Amazon S3 버킷에 저장할 수 있습니다. 사용 가능한 권한에는 두 가지 수준이 있습니다.

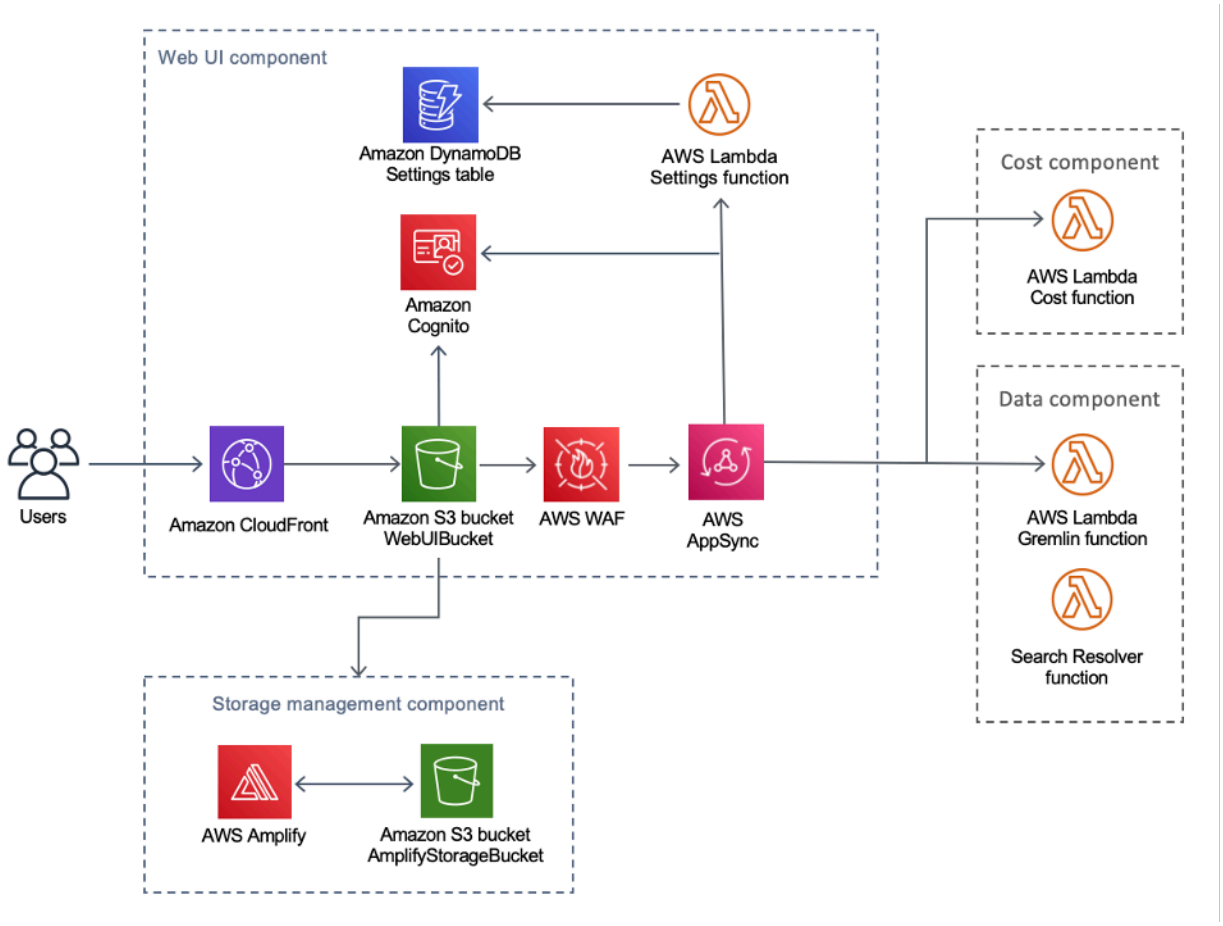
- 모든 사용자 - 배포의 AWS 사용자에 대한 워크로드 검색에서 AWS 아키텍처 다이어그램을 볼 수 있도록 허용합니다. 사용자는 이러한 다이어그램을 다운로드하고 편집할 수 있습니다.
- 사용자 - AWS 아키텍처 다이어그램의 워크로드 검색을 생성자만 볼 수 있도록 허용합니다. 다른 사용자는 볼 수 없습니다.

## 웹 UI 및 스토리지 관리

React를 사용하여 웹 UI를 개발했습니다. 웹 UI는 사용자가 AWS의 워크로드 검색과 상호 작용할 수 있는 프런트엔드 콘솔을 제공합니다.

Amazon CloudFront는 웹 UI에 대한 모든 HTTP 요청에 보안 헤더를 추가하도록 구성되어 있습니다. 이를 통해 추가 보안 계층을 제공하여 교차 사이트 스크립팅(XSS)과 같은 공격으로부터 보호합니다.

AWS 웹 UI 및 스토리지 관리 구성 요소의 워크로드 검색

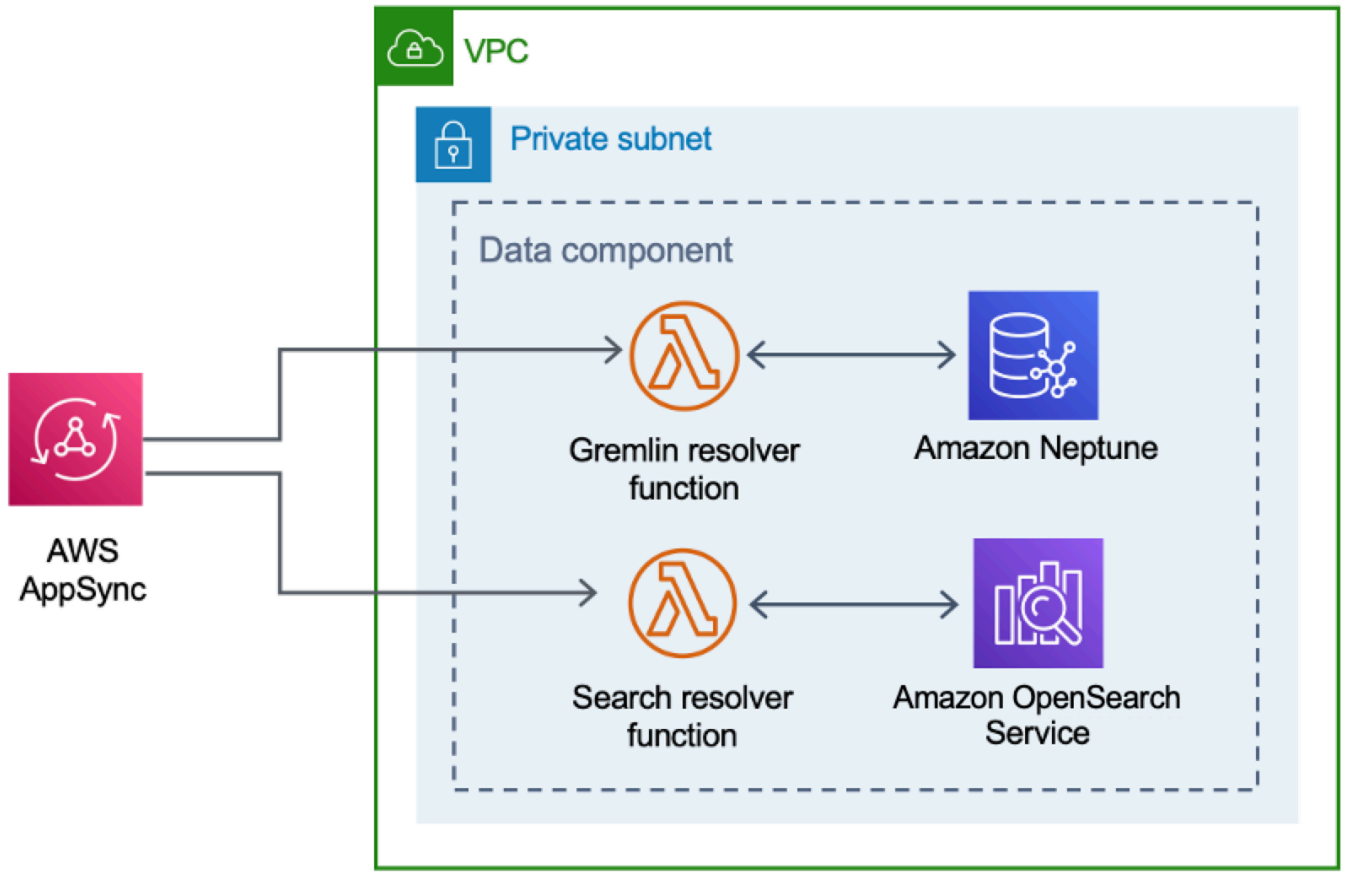



웹 UI 리소스는 `WebUIBucket` Amazon S3 버킷에서 호스팅되고 Amazon CloudFront에서 배포됩니다. AWS Amplify는 AWS AppSync 및 Amazon S3에 대한 통합을 간소화하는 추상화 계층을 제공합니다.

이 솔루션은 AWS AppSync를 사용하여 가져온 리전 관리를 포함하여 AWS에서 워크로드 검색에 사용할 수 있는 다양한 구성과의 상호 작용을 용이하게 합니다. AWS AppSync는 `Settings` AWS Lambda 함수를 사용하여 새 계정 또는 리전 가져오기와 같은 요청을 처리합니다.

# 데이터 구성 요소

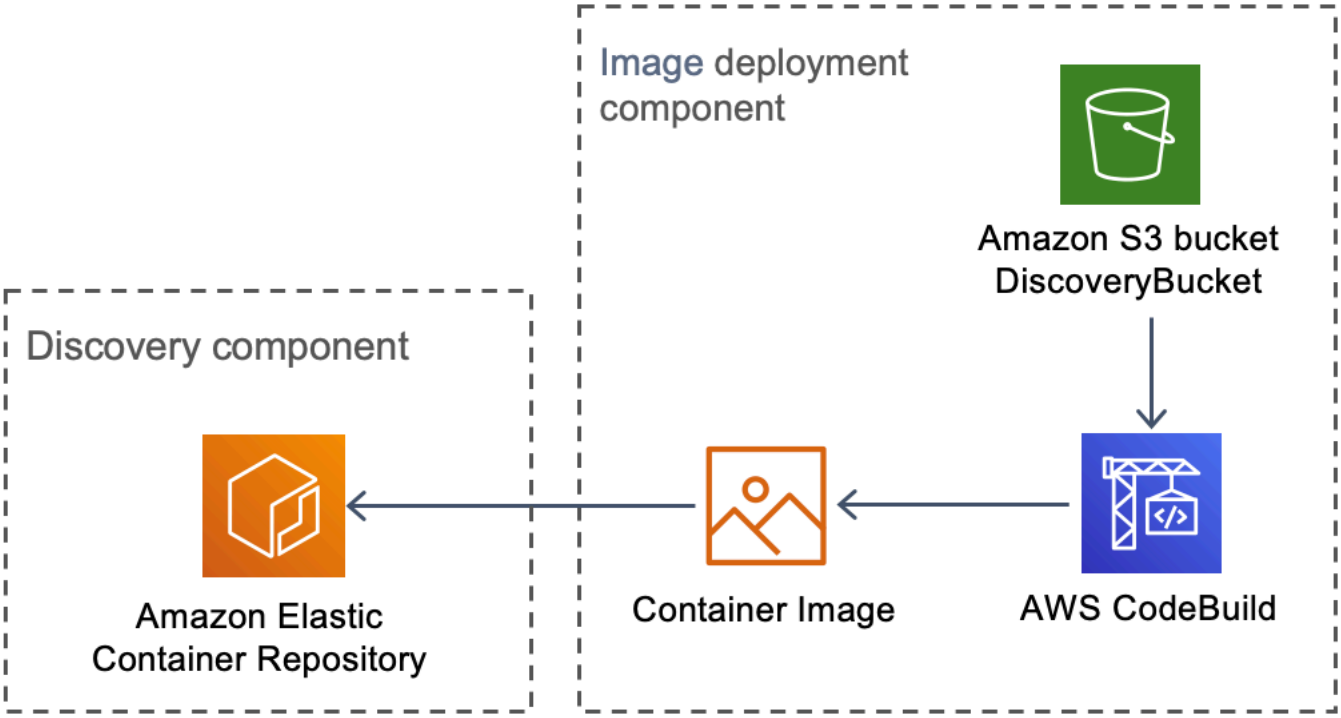
AWS 데이터 구성 요소의 워크로드 검색




웹 UI는 AppSync API로 요청을 전송하여 `Gremlin Resolver` 또는 `Search Resolver` Lambda 함수를 호출합니다. 이러한 함수는 요청을 처리하고 Amazon Neptune 또는 OpenSearch Service를 쿼리하여 제공된 리소스에 대한 데이터를 검색합니다. 또한 AWS AppSync는 AWS CUR의 예상 비용 데이터에 대한 요청을 지원합니다.

검색 구성 요소는 AppSync API로 요청을 전송하여 Amazon Neptune 및 OpenSearch Service 데이터베이스의 데이터를 읽고 유지합니다. API는 검색 구성 요소의 AWS Fargate 작업에서 요청을 수신합니다. 그런 다음 API는 데이터베이스에 대한 액세스를 제공하는 IAM 역할을 사용하여 인증됩니다.

# 이미지 배포 구성 요소



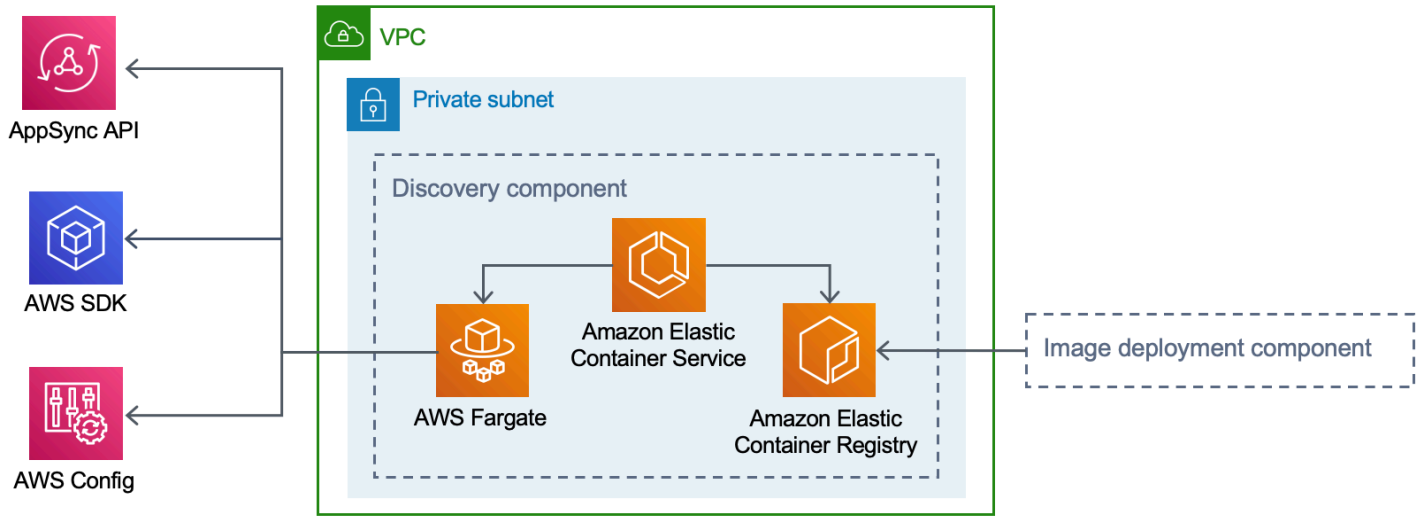

AWS 이미지 배포 구성 요소의 워크로드 검색

이미지 배포 구성 요소는 검색 구성 요소가 사용하는 컨테이너 이미지를 빌드합니다. `DiscoveryBucket` 및 Amazon S3 버킷은 컨테이너 이미지를 빌드하고 Amazon ECR에 업로드하는 AWS CodeBuild 작업에 의해 배포 시 다운로드할 수 있는 코드를 호스팅합니다.

# 검색 구성 요소

검색 구성 요소는 AWS 아키텍처에서 워크로드 검색의 주요 데이터 수집 요소입니다. AWS Config를 쿼리하고 API 호출을 설명하여 리소스 인벤토리와 리소스 간의 관계를 유지하는 것은 AWS Config의 책임입니다.

AWS 검색 구성 요소의 워크로드 검색



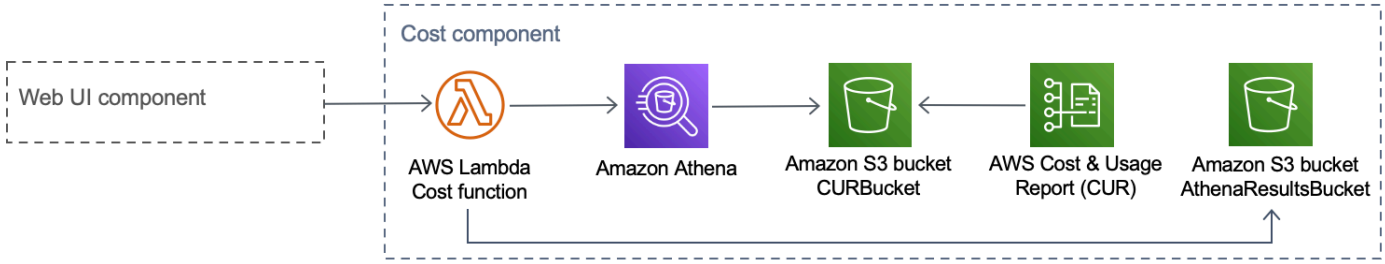

이 솔루션은 Amazon ECR에서 다운로드한 컨테이너 이미지를 사용하여 AWS Fargate 작업을 실행하도록 Amazon ECS를 구성합니다. AWS Fargate 작업은 15분 간격으로 실행되도록 예약되어 있습니다. 수집된 리소스 관계 데이터는 Amazon Neptune 그래프 데이터베이스 및 Amazon OpenSearch Service에 삽입됩니다.

검색 구성 요소 워크플로는 다음 세 단계로 구성됩니다.

1. Amazon ECS는 15분 간격으로 AWS Fargate 작업을 호출합니다.
2. Fargate 태스크는 AWS Config, AWS API 설명 호출 및 Amazon Neptune 데이터베이스에서 리소스 데이터를 수집합니다.
3. Fargate 작업은 Amazon Neptune 데이터베이스에 있는 항목과 AWS Config에서 수신한 항목 및 설명 호출 간의 차이를 계산합니다.
4. Fargate 태스크는 AppSync API에 요청을 전송하여 Amazon Neptune 및 Amazon OpenSearch Service에서 검색된 리소스 및 관계의 변경 사항을 유지합니다.

# 비용 구성 요소

AWS 비용 구성 요소의 워크로드 검색




AWS Billing and Cost Management and Cost Management에서 AWS CUR을 생성할 수 있습니다. 이렇게 하면 Parquet 형식의 파일이 `CostAndUsageReportBucket` Amazon S3 버킷에 게시됩니다. 웹 UI는 Cost Lambda 함수를 호출하는 AWS AppSync 엔드포인트에 요청합니다. 함수는 AWS CUR에서 예상 비용 정보를 반환하는 사전 정의된 쿼리를 Amazon Athena로 보냅니다.

AWS CUR의 크기로 인해 Amazon Athena의 응답이 매우 클 수 있습니다. 솔루션은 결과를 `AthenaResultsBucket` Amazon S3 버킷에 저장하고 결과를 웹 UI로 다시 페이지 매김합니다. 이 버킷에 구성된 수명 주기 정책은 7일이 지난 항목을 제거합니다.

# 이 솔루션의 AWS 서비스

| AWS 서비스 | 설명 |
| --- | --- |
| AppSync | Core. 이 솔루션은 AppSync를 사용하여 웹 UI가 사용하는 서버리스 GraphQL API를 제공합니다. |
| Amazon CloudFront | Core. 이 솔루션은 Amazon S3 버킷이 오리진인 CloudFront를 사용합니다. 이렇게 하면 Amazon S3 버킷에 대한 액세스가 제한되어 공개적으로 액세스할 수 없으며 버킷으로부터의 직접 액세스를 방지할 수 있습니다. |
| Config | Core. 솔루션은 AWS Config를 솔루션이 검색하는 리소스 및 관계의 기본 데이터 소스로 사용합니다. |
| Amazon OpenSearch Service | Core. 이 솔루션은 애플리케이션 모니터링, 로그 분석 및 관찰성을 위해 Amazon OpenSearch Service를 사용합니다. |

| AWS 서비스 | 설명 |
| --- | --- |
| Amazon DynamoDB | Core. 이 솔루션은 DynamoDB를 사용하여 솔루션의 구성 데이터를 저장합니다. |
| Amazon Elastic Container Service(ECS) | Core. 이 솔루션은 Amazon ECS를 사용하여 AWS 계정에서 리소스 및 관계를 검색하는 작업 실행을 오케스트레이션합니다. |
| AWS Fargate | Core. 이 솔루션은 Amazon ECS의 AWS Fargate를 검색 작업의 컴퓨팅 계층으로 사용합니다. |
| Lambda | Core. 이 솔루션은 Node.js 및 Python 런타임과 함께 서버리스 Lambda 함수를 사용하여 API 호출을 처리합니다. |
| Amazon Neptune | Core. 이 솔루션은 Neptune을 솔루션이 검색하는 리소스 및 관계에 대한 기본 데이터 스토어로 사용합니다. |
| Amazon Simple Storage Service(S3) | Core. 이 솔루션은 프런트엔드 및 백엔드 스토리지 목적으로 Amazon S3를 사용합니다. |
| Amazon CloudWatch | 지원. 이 솔루션은 CloudWatch를 사용하여 자동화된 사례에서 실시간 로그, 지표 및 이벤트 데이터를 수집하고 시각화합니다. 또한 배포된 솔루션의 리소스 사용량 및 성능 문제를 모니터링할 수 있습니다. |
| AWS CodeBuild | 지원. 이 솔루션은 CodeBuild를 사용하여 검색 작업용 코드가 포함된 Docker 컨테이너를 빌드하고 프런트엔드의 자산을 Amazon S3에 배포합니다. |
| Amazon Cognito | 지원. 이 솔루션은 Cognito 사용자 풀을 사용하여 사용자가 솔루션 웹 UI에 액세스할 수 있도록 인증하고 권한을 부여합니다. |

| AWS 서비스 | 설명 |
| --- | --- |
| AWS Systems Manager | 지원. 이 솔루션은 AWS Systems Manager를 사용하여 애플리케이션 수준의 리소스 모니터링과 리소스 작업 및 비용 데이터의 시각화를 제공합니다. |
| Amazon Virtual Private Cloud | 지원. 이 솔루션은 VPC를 사용하여 Neptune 및 OpenSearch 데이터베이스를 시작합니다. |
| AWS WAF | 지원. 이 솔루션은 AWS WAF를 사용하여 가용성에 영향을 미치거나 보안을 손상시키거나 과도한 리소스를 소비할 수 있는 일반적인 악용 및 봇으로부터 AppSync API를 보호합니다. |
| Amazon Athena | 선택 사항. 이 솔루션은 비용 기능이 활성화된 경우 Athena를 사용하여 비용 및 사용 보고서를 쿼리합니다. |

# 배포 계획

이 섹션에서는 솔루션을 배포하기 전에 리전, 비용, 보안 및 기타 고려 사항을 설명합니다.

## 지원되는 AWS 리전

이 솔루션은 현재 일부 AWS 리전에서 사용할 수 없는 Amazon Cognito 서비스를 사용합니다. 리전별 AWS 서비스의 최신 가용성은 AWS 리전 서비스 목록을 참조하세요.

AWS의 워크로드 검색은 다음 AWS 리전에서 사용할 수 있습니다.

| 리전 이름 | |
|---|---|
| 미국 동부(버지니아 북부) | 캐나다(중부) |
| 미국 동부(오하이오) | 유럽(런던) |
| 미국 서부(오리건) | 유럽(프랑크푸르트) |
| 아시아 태평양(뭄바이) | 유럽(아일랜드) |
| 아시아 태평양(서울) | 유럽(파리) |
| 아시아 태평양(싱가포르) | 유럽(스톡홀름) |
| 아시아 태평양(시드니) | 남아메리카(상파울루) |
| 아시아 태평양(도쿄) | |

AWS의 워크로드 검색은 다음 AWS 리전에서 사용할 수 없습니다.

| 리전 이름 | 사용할 수 없는 서비스 |
|---|---|
| AWS GovCloud(US-East) | AppSync |
| AWS GovCloud (US-West) | AppSync |
| 중국(베이징) | Amazon Cognito |

| 리전 이름 | 사용할 수 없는 서비스 |
| --- | --- |
| 중국(닝샤) | Amazon Cognito |

# 비용

이 솔루션을 실행하는 동안 프로비저닝된 AWS 서비스의 비용은 사용자의 책임입니다. 이 개정부터 미국 동부(버지니아 북부) 리전에서 단일 인스턴스 배포 옵션을 사용하여이 솔루션을 실행하는 데 드는 비용은 시간당 약 0.58 USD 또는 월 425.19 USD입니다.

> **Note**
>
> AWS 클라우드에서 AWS에서 워크로드 검색을 실행하는 데 드는 비용은 선택한 배포 구성에 따라 달라집니다. 다음 예제에서는 미국 동부(버지니아 북부) 리전의 단일 인스턴스 및 여러 인스턴스 배포 구성에 대한 비용 분석을 제공합니다. 아래 예제 테이블에 나열된 AWS 서비스는 월별로 요금이 청구됩니다.

비용 관리에 도움이 되도록 AWS Cost Explorer를 통해 예산을 생성하는 것이 좋습니다. 요금은 변경될 수 있습니다. 자세한 내용은이 솔루션에 사용되는 각 AWS 서비스의 요금 웹 페이지를 참조하세요.

## 비용 테이블 예

### 옵션 1: 단일 인스턴스 배포(기본값)

AWS CloudFormation 템플릿을 사용하여이 솔루션을 배포할 때 OpensearchMultiAz 파라미터를 수정하여 OpenSearch Service 도메인에 대한 단일 인스턴스를 No 배포하고 CreateNeptuneReplica 파라미터를 수정하여 Neptune 데이터 스토어에 대한 단일 인스턴스를 No 배포합니다. 단일 인스턴스 배포 옵션은 더 낮은 비용을 발생시키지만 가용 영역에 장애가 발생할 경우 AWS에서 워크로드 검색의 가용성을 줄입니다.

| AWS 서비스 | 인스턴스 유형 | 시간당 비용[USD] | 월별 비용[USD] |
| --- | --- | --- | --- |
| Amazon Neptune | `db.r5.large` | 0.348 USD | 254.04 USD |
| Amazon OpenSearch Service | `m6g.large.search` | 0.128 USD | 93.44 USD |

| AWS 서비스 | 인스턴스 유형 | 시간당 비용[USD] | 월별 비용[USD] |
| --- | --- | --- | --- |
| Amazon VPC(NAT 게이트웨이) | N/A | 0.090 USD | 65.7 USD |
| Config | N/A | 리소스당 0.003 USD | 리소스당 0.003 USD |
| Amazon ECS(AWS Fargate 작업) | N/A | 0.02 USD | 12.01 USD |
| 합계 | | 0.586 USD | 425.19 USD |

## 옵션 2: 여러 인스턴스 배포

AWS CloudFormation 템플릿을 사용하여이 솔루션을 배포할 때 OpensearchMultiAz 파라미터를 수정하여 OpenSearch Service 도메인의 두 가용 영역에 두 개의 인스턴스를 `Yes` 배포하고 CreateNeptuneReplica 파라미터를 수정하여 Neptune 데이터 스토어의 두 가용 영역에 두 개의 인스턴스를 `Yes` 배포합니다. 여러 인스턴스 배포 옵션을 실행하면 실행 비용이 더 많이 들지만 가용 영역에 장애가 발생할 경우 AWS에서 워크로드 검색의 가용성이 높아집니다.

| AWS 서비스 | 인스턴스 유형 | 시간당 비용 | 월별 비용[USD] |
| --- | --- | --- | --- |
| Amazon Neptune | `db.r5.large` | 0.696 USD | 508.08 USD |
| Amazon OpenSearch Service | `m6g.large.search` | 0.256 USD | 186.88 USD |
| Amazon VPC(NAT 게이트웨이) | N/A | 0.090 USD | 65.7 USD |
| Config | N/A | 리소스당 0.003 USD | 리소스당 0.003 USD |
| Amazon ECS(AWS Fargate 작업) | N/A | 0.02 USD | 12.01 USD |
| 합계 | | 1.062 USD | 772.67 USD |

- 최종 비용은 AWS Config가 감지하는 리소스 수에 따라 달라집니다. 테이블에 제공된 금액 외에 기록된 리소스 항목당 0.003 USD가 발생합니다.

> **Important**
>
> Amazon Neptune 및 Amazon OpenSearch Service 비용은 선택한 인스턴스 유형에 따라 달라집니다.

# 보안

AWS 인프라에 시스템을 구축하면 사용자와 AWS 간에 보안 책임이 공유됩니다. AWS는 호스트 운영 체제, 가상화 계층, 서비스가 운영되는 시설의 물리적 보안을 비롯한 구성 요소를 운영, 관리 및 제어하므로이 공동 책임 모델은 운영 부담을 줄입니다. AWS 보안에 대한 자세한 내용은 AWS 보안 센터를 참조하십시오.

## 리소스 액세스

### IAM 역할

IAM 역할을 통해 고객은 AWS 클라우드의 서비스 및 사용자에게 세분화된 액세스 정책 및 권한을 할당할 수 있습니다. AWS에서 워크로드 검색을 실행하고 AWS 계정에서 리소스를 검색하려면 여러 역할이 필요합니다.

### Amazon Cognito

Amazon Cognito는 AWS의 워크로드 검색에 필요한 구성 요소에 대한 액세스 권한을 부여하는 수명이 짧고 강력한 자격 증명을 사용하여 액세스를 인증하는 데 사용됩니다.

## 네트워크 액세스

### Amazon VPC

AWS의 워크로드 검색은 Amazon VPC 내에 배포되고 보안 및 고가용성을 제공하기 위한 모범 사례에 따라 구성됩니다. 자세한 내용은 VPC의 보안 모범 사례를 참조하세요. VPC 엔드포인트는 서비스 간 비인터넷 전송을 허용하며 사용 가능한 경우 구성됩니다.

보안 그룹은 AWS에서 워크로드 검색을 실행하는 데 필요한 구성 요소 간의 네트워크 트래픽을 제어하고 격리하는 데 사용됩니다.

배포가 시작되고 실행되면 보안 그룹을 검토하고 필요에 따라 액세스를 추가로 제한하는 것이 좋습니다.

### Amazon CloudFront

이 솔루션은 Amazon CloudFront에서 배포하는 Amazon S3 버킷에 호스팅된 웹 콘솔 UI를 배포합니다. Amazon CloudFront 오리진 액세스 ID 기능을 사용하면이 Amazon S3 버킷의 콘텐츠에 CloudFront를 통해서만 액세스할 수 있습니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한을 참조하세요. Amazon CloudFront

CloudFront는 추가 보안 완화를 활성화하여 각 최종 사용자 응답에 HTTP 보안 헤더를 추가합니다. 자세한 내용은 CloudFront 응답에서 HTTP 헤더 추가 또는 제거를 참조하세요.

이 솔루션은 TLS v1.0의 최소 지원 보안 프로토콜이 있는 기본 CloudFront 인증서를 사용합니다. TLS v1.2 또는 TLS v1.3 사용을 적용하려면 기본 CloudFront 인증서 대신 사용자 지정 SSL 인증서를 사용해야 합니다. 자세한 내용은 SSL/TLS 인증서를 사용하도록 CloudFront 배포를 구성하려면 어떻게 해야 하나요?를 참조하세요.

## 애플리케이션 구성

### AppSync

AWS GraphQL APIs의 워크로드 검색에는 GraphQL 사양에 따라 AWS AppSync에서 제공하는 요청 검증이 있습니다. 또한 인증 및 권한 부여는 사용자가 웹 UI에서 성공적으로 인증할 때 Amazon Cognito에서 제공하는 JWT를 사용하는 IAM 및 Amazon Cognito를 사용하여 구현됩니다.

### AWS Lambda

기본적으로 Lambda 함수는 언어 런타임의 가장 안정적인 최신 버전으로 구성됩니다. 민감한 데이터나 보안 암호는 로깅되지 않습니다. 서비스 상호 작용은 최소 필수 권한으로 수행됩니다. 이러한 권한을 정의하는 역할은 함수 간에 공유되지 않습니다.

### Amazon OpenSearch Service

Amazon OpenSearch Service 도메인은 OpenSearch Service 클러스터에 대한 서명되지 않은 요청을 중지하도록 액세스를 제한하는 액세스 정책으로 구성됩니다. 이는 단일 Lambda 함수로 제한됩니다.

OpenSearch Service 클러스터는 기존 OpenSearch Service 보안 기능 외에도 추가 데이터 보호 계층을 추가하기 위해 node-to-node 암호화가 활성화된 상태로 구축됩니다.

# 할당량

서비스 할당량(제한이라고도 함)은 AWS 계정의 최대 서비스 리소스 또는 작업 수입니다.

## 이 솔루션의 AWS 서비스 할당량

이 솔루션에 구현된 각 서비스의 할당량이 충분한지 확인하세요. 자세한 내용은 AWS 서비스 할당량을 참조하세요.

다음 링크를 사용하여 해당 서비스의 페이지로 이동합니다. 페이지를 전환하지 않고 설명서의 모든 AWS 서비스에 대한 서비스 할당량을 보려면 대신 PDF의 서비스 엔드포인트 및 할당량 페이지에서 정보를 확인합니다.

| | |
|---|---|
| Amplify | Amazon ECR |
| 아테나 | Lambda |
| CloudFront | OpenSearch 서비스 |
| Cognito | Neptune |
| 구성 | Amazon S3 |
| Amazon ECS | |

## AWS CloudFormation 할당량

AWS 계정에는이 솔루션에서 스택을 시작할 때 알아야 할 AWS CloudFormation 할당량이 있습니다. 이러한 할당량을 이해하면 이 솔루션을 성공적으로 배포하지 못하는 제한 오류를 방지할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의에서 AWS CloudFormation 할당량을 참조하세요 AWS CloudFormation.

## AWS Lambda 할당량

계정의 AWS Lambda 동시 실행 할당량은 1000입니다. Lambda를 실행하고 사용하는 다른 워크로드가 있는 계정에서 솔루션을 사용하는 경우이 할당량을 적절한 값으로 설정합니다. 이 값은 조정할 수 있습니다. 자세한 내용은 AWS Lambda 사용 설명서의 AWS Lambda 할당량을 참조하세요 AWS Lambda.

> **Note**
>
> 이 솔루션을 배포하려는 계정에서 동시 실행 할당량에서 150개의 실행을 사용할 수 있어야 합니다. 해당 계정에서 사용 가능한 실행이 150개 미만인 경우 CloudFormation 배포가 실패합니다.

## Amazon VPC 할당량

AWS 계정에는 VPCs개와 탄력적 IPs(EIPs. 다른 VPCs 또는 EIPs가 있는 계정에서 솔루션을 사용하는 경우이 솔루션을 성공적으로 배포하지 못할 수 있습니다. 이 할당량에 도달할 위험이 있는 경우 스택 시작 섹션의 단계를 따를 때 VPC를 제공하여 배포를 위한 자체 VPC를 제공할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC 할당량을 참조하세요.

# 배포 계정 선택

AWS에서 워크로드 검색을 AWS Organization에 배포하는 경우 StackSets 및 다중 리전 AWS Config 기능이 활성화된 위임된 관리자 계정에 솔루션을 설치해야 합니다.

AWS Organizations를 사용하지 않는 경우 AWS에서 워크로드 검색을이 솔루션을 위해 특별히 생성된 전용 AWS 계정에 배포하는 것이 좋습니다. 이 접근 방식은 AWS의 워크로드 검색이 기존 워크로드와 격리되어 있으며 사용자 추가 및 새 리전 가져오기와 같은 솔루션을 구성할 수 있는 단일 위치를 제공합니다. 또한 솔루션을 실행하는 동안 발생하는 비용을 더 쉽게 추적할 수 있습니다.

AWS에서 워크로드 검색을 배포한 후 이미 프로비저닝한 계정에서 리전을 가져올 수 있습니다.

# 솔루션 배포

이 솔루션은 AWS CloudFormation 템플릿 및 스택을 사용하여 배포를 자동화합니다. CloudFormation 템플릿은이 솔루션에 포함된 AWS 리소스와 해당 속성을 지정합니다. CloudFormation 스택은 템플릿에 설명된 리소스를 프로비저닝합니다.

## 배포 프로세스 개요

> **Note**
>
> 이전에 AWS에 워크로드 검색을 배포했고 최신 버전으로 업그레이드하려는 경우 솔루션 업데이트를 참조하세요.

이 섹션의 step-by-step 지침에 따라 솔루션을 구성하고 계정에 배포합니다.

배포 시간: 약 30분

솔루션을 시작하기 전에이 가이드에서 설명하는 비용, 아키텍처, 네트워크 보안 및 기타 고려 사항을 검토하세요.

> **Important**
>
> 이 솔루션에는 익명화된 운영 지표를 AWS로 전송하는 옵션이 포함되어 있습니다. 당사는 이 데이터를 사용하여 고객이 이 솔루션과 관련 서비스 및 제품을 어떻게 사용하는지 더 잘 이해합니다. AWS는이 설문 조사를 통해 수집된 데이터를 소유합니다. 데이터 수집에는 AWS 개인 정보 보호 고지가 적용됩니다.

## 사전 조건

### 배포 파라미터 세부 정보 수집

AWS에 워크로드 검색을 배포하기 전에 Amazon OpenSearch Service 서비스 연결 역할 및 AWS Config에 대한 구성 세부 정보를 검토합니다.

## AWSServiceRoleForAmazonOpenSearchService 역할이 있는지 확인

배포는 Amazon Virtual Private Cloud(Amazon VPC) 내에 Amazon OpenSearch Service 클러스터를 생성합니다. 템플릿은 서비스 연결 역할을 사용하여 OpenSearch Service 클러스터를 생성합니다. 그러나 계정에 이미 역할이 생성된 경우 기존 역할을 사용합니다.

이 역할이 이미 있는지 확인하려면:

1. 이 솔루션을 배포하려는 계정의 Identity and Access Management(IAM) 콘솔에 로그인합니다.
2. 검색 상자에를 입력합니다`AWSServiceRoleForAmazonOpenSearchService`.
3. 검색에서 역할을 반환하는 경우 스택을 시작할 때 CreateOpensearchServiceRole 파라미터에 No 대해를 선택합니다.

## AWS Config가 설정되었는지 확인

AWS의 워크로드 검색은 AWS Config를 사용하여 대부분의 리소스 구성을 수집합니다. 솔루션을 배포하거나 새 리전을 가져올 때 AWS Config가 이미 설정되어 있고 예상대로 작동하는지 확인해야 합니다. AlreadyHaveConfigSetup CloudFormation 파라미터는 AWS Config를 설정할지 여부를 AWS의 워크로드 검색에 알립니다.

AWS CLI 명령 참조에서 가져온 코드 조각은 다음과 같습니다. AWS에서 워크로드 검색을 배포하거나 AWS에서 워크로드 검색으로 가져오려는 리전에서 명령을 실행합니다.

다음 명령을 입력합니다.

```
aws configservice get-status
```

출력과 유사한 응답을 수신하면 해당 리전에서 실행 중인 구성 레코더 및 전송 채널이 있습니다. AlreadyHaveConfigSetup CloudFormation 파라미터에 `Yes` 대해를 선택합니다.

출력:

```
Configuration Recorders:

name: default
recorder: ON
last status: SUCCESS

Delivery Channels:
```

```
name: default
last stream delivery status: SUCCESS
last history delivery status: SUCCESS
last snapshot delivery status: SUCCESS
```

AWS CloudFormation StackSets를 구성하는 경우 AWS Config가 이미 구성된 리전 배치에이 리전을 포함해야 합니다.

## 계정에서 AWS Config 세부 정보 확인

배포는 AWS Config 설정을 시도합니다. AWS에서 워크로드 검색을 통해 배포하거나 검색할 수 있도록 하려는 계정에서 AWS Config를 이미 사용하고 있는 경우이 솔루션을 배포할 때 관련 파라미터를 선택합니다. 또한 배포에 성공하려면 AWS Config가 스캔하는 리소스를 제한하지 않았는지 확인합니다.

현재 AWS Config 구성을 확인하려면:

1. AWS Config 콘솔에 로그인합니다.
2. 설정을 선택하고 이 리전에서 지원되는 모든 리소스 기록 및 글로벌 리소스 포함 상자가 선택되어 있는지 확인합니다.

## VPC 구성 확인

기존 VPC에 배포하는 경우 프라이빗 서브넷이 AWS 서비스로 요청을 라우팅할 수 있는지 확인합니다.

기존 VPC에 솔루션을 배포하는 옵션을 선택하는 경우 AWS Lambda에서 워크로드 검색 함수와 VPC의 프라이빗 서브넷에서 실행되는 Amazon ECS 태스크가 다른 AWS 서비스에 연결할 수 있는지 확인해야 합니다. 이를 활성화하는 표준 방법은 NAT 게이트웨이를 사용하는 것입니다. 다음 코드 샘플과 같이 계정의 NAT 게이트웨이를 나열할 수 있습니다.

```
aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<private-
subnet-id1>,<private-subnet-id2> --query 'RouteTables[].Routes[].NatGatewayId'
```

출력:

```
[
    "nat-1111111111111111",
    "nat-2222222222222222"
```

```
]
```

> **Note**
> 결과가 2개 미만이면 서브넷에 올바른 수의 NAT 게이트웨이가 없는 것입니다.

VPC에 NAT 게이트웨이가 없는 경우 이를 프로비저닝하거나 AWS APIs 섹션에 나열된 모든 AWS 서비스에 대한 VPC 엔드포인트가 있는지 확인해야 합니다.

## AWS CloudFormation 템플릿

이 솔루션은 AWS CloudFormation을 사용하여 AWS 클라우드의 AWS에서 워크로드 검색 배포를 자동화합니다. 여기에는 배포 전에 다운로드할 수 있는 다음 CloudFormation 템플릿이 포함되어 있습니다.

**View template**

workload-discovery-on-aws.template -이 템플릿을 사용하여 솔루션 및 모든 관련 구성 요소를 시작합니다. 기본 구성은 이 솔루션 섹션의 AWS 서비스에 있는 코어 및 지원 솔루션을 배포하지만 특정 요구 사항에 맞게 템플릿을 사용자 지정할 수 있습니다.

> **Note**
> 특정 요구 사항에 맞게 템플릿을 사용자 지정할 수 있지만 변경 사항이 업그레이드 프로세스에 영향을 미칠 수 있습니다.

## 스택 시작

이 자동화된 AWS CloudFormation 템플릿은 AWS 클라우드의 AWS에 워크로드 검색을 배포합니다. 스택을 시작하기 전에 배포 파라미터 세부 정보를 수집해야 합니다. 자세한 내용은 사전 조건을 참조하세요.

배포 시간: 약 30분

1. AWS Management Console에 로그인하고 버튼을 선택하여 `workload-discovery-on-aws.template` AWS CloudFormation 템플릿을 시작합니다.

Launch solution

2. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른 AWS 리전에서 솔루션을 시작하려면 콘솔 탐색 모음에서 리전 선택기를 사용합니다.

> **Note**
>
> 이 솔루션은 일부 AWS 리전에서 사용할 수 없는 서비스를 사용합니다. 지원되는 AWS 리전 목록은 지원되는 AWS 리전을 참조하세요.

3. 스택 생성 페이지에서 Amazon S3 URL 텍스트 상자에 올바른 템플릿 URL이 있는지 확인하고 다음을 선택합니다.
4. 스택 세부 정보 지정 페이지에서 솔루션 스택 이름을 할당합니다. 문자 제한 이름 지정에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 및 AWS STS 할당량을 참조하세요. AWS Identity and Access Management
5. 파라미터에서이 솔루션 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

| 파라미터 | Default | 설명 |
| --- | --- | --- |
| AdminUserEmailAddress | *<## ##>* | 첫 번째 사용자를 생성할 이메일 주소입니다. 임시 자격 증명이이 이메일 주소로 전송됩니다. |
| AlreadyHaveConfigSetup | No | 배포 계정에 AWS Config가 이미 설정되어 있는지 여부를 확인합니다. 자세한 내용은 사전 조건을 참조하세요. |
| AthenaWorkgroup | `primary` | 비용 기능이 활성화된 경우 Athena 쿼리를 발행하는 데 사용할 작업 그룹입니다. |
| ApiAllowListedRanges | `0.0.0.0/1,128.0.0.0/1` | AppSync GraphQL API에 대한 액세스를 관리하기 위해 쉼 |

| 파라미터 | Default | 설명 |
| --- | --- | --- |
| | | 표로 구분된 CIDRs. 전체 인터넷을 허용하려면 0.0.0.0/1,128.0.0.0/1을 사용합니다. 특정 CIDRs에 대한 액세스를 제한하는 경우 프라이빗 서브넷에서 실행되는 검색 프로세스 ECS 작업이 인터넷에 액세스할 수 있도록 허용하는 NAT 게이트웨이의 IP 주소(및 /32의 서브넷 마스크)도 포함해야 합니다. 참고:이 허용 목록은 WebUI에 대한 액세스를 제어하지 않고 GraphQL API만 제어합니다. |
| CreateNeptuneReplica | No | 별도의 가용 영역에서 Neptune에 대한 읽기 전용 복제본을 생성할지 여부를 선택합니다. 선택하면 복원력이 Yes 향상되지만이 솔루션의 비용은 증가합니다. |
| CreateOpenSearchServiceRole | Yes | Amazon OpenSearch Service에 대한 서비스 연결 역할이 이미 있는지 여부를 확인합니다. 자세한 내용은 사전 조건을 참조하세요. |
| NeptuneInstanceClass | db.r5.large | Amazon Neptune 데이터베이스를 호스팅하는 데 사용되는 인스턴스 유형입니다. 여기에서 선택하는 항목은이 솔루션 실행 비용에 영향을 미칩니다. |

| 파라미터 | Default | 설명 |
| --- | --- | --- |
| OpensearchInstanceType | `m6g.large.search` | OpenSearch Service 데이터 노드에 사용되는 인스턴스 유형입니다. 선택한 항목은 솔루션 실행 비용에 영향을 미칩니다. |
| OpensearchMultiAz | No | 여러 가용 영역에 걸쳐 OpenSearch Service 클러스터를 생성할지 여부를 선택합니다. 선택하면 복원력이 `Yes` 향상되지만이 솔루션의 비용은 증가합니다. |
| CrossAccountDiscovery | `SELF_MANAGED` | AWS 또는 AWS Organizations에서 워크로드 검색을 통해 계정 가져오기를 관리할지 여부를 선택합니다. `SELF_MANAGED` 또는 `AWS_ORGANIZATIONS` 값을 가질 수 있습니다. |
| OrganizationUnitId | <선택 사항 입력> | 루트 조직 단위 ID입니다. 이 파라미터는 CrossAccountDiscovery가 로 설정된 경우에만 사용됩니다`AWS_ORGANIZATIONS` . |
| AccountType | `DELEGATED_ADMIN` | AWS에 워크로드 검색을 설치할 AWS Organizations 계정의 유형입니다. 이 파라미터는 CrossAccountDiscovery가 로 설정된 경우에만 사용됩니다`AWS_ORGANIZATIONS` . 자세한 내용은 배포 계정 선택을 참조하세요. |

| 파라미터 | Default | 설명 |
| --- | --- | --- |
| ConfigAggregatorName | <선택 사항 입력> | 사용할 AWS 조직 전체 Config 집계자입니다. 이 애그리게이터와 동일한 계정 및 리전에 솔루션을 설치해야 합니다. 이 파라미터를 비워 두면 새 집계자가 생성됩니다. 이 파라미터는 CrossAccountDiscovery가로 설정된 경우에만 사용됩니다`AWS;_ORGANIZATIONS` . |
| CpuUnits | `1 vCPU` | 검색 프로세스가 실행되는 Fargate 작업에 할당할 CPUs 수입니다. |
| 메모리 | `2048` | 검색 프로세스가 실행되는 Fargate 작업에 할당할 메모리의 양입니다. |
| DiscoveryTaskFrequency | `15mins` | 검색 프로세스 ECS 작업을 실행할 때마다의 시간 간격입니다. |
| MinNCUs | 1 | Neptune 클러스터에 설정할 최소 Neptune 용량 단위(NCUs)입니다(MaxNCUs보다 작거나 같아야 함). DBInstance 유형이 인 경우 필수입니다`db.serverless` . |
| MaxNCUs | `128` | Neptune 클러스터에서 설정할 최대 NCUs입니다(MinNCUs 이상이어야 함). DBInstance 유형이 인 경우 필수입니다`db.serverless` . |

| 파라미터 | Default | 설명 |
| --- | --- | --- |
| VpcId | <선택 사항 입력> | 솔루션이 사용할 기존 VPC의 ID입니다. 이 파라미터를 비워 두면 새 VPC가 프로비저닝됩니다. |
| VpcCidrBlock | <선택 사항 입력> | VpcId 파라미터에서 참조하는 VPC의 VPC CIDR 블록입니다. 이 파라미터는 VpcId 파라미터가 설정된 경우에만 사용됩니다. |
| PrivateSubnet0 | <선택 사항 입력> | 사용하려는 프라이빗 서브넷입니다. 이 파라미터는 VpcId 파라미터가 설정된 경우에만 사용됩니다. |
| PrivateSubnet1 | <선택 사항 입력> | 사용하려는 프라이빗 서브넷입니다. 이 파라미터는 VpcId 파라미터가 설정된 경우에만 사용됩니다. |
| UsesCustomIdentity | No | SAML 또는 OIDC와 같은 사용자 지정 자격 증명 공급자를 사용할지 여부를 확인합니다. |
| CognitoCustomDomain | <선택 사항 입력> | 애플리케이션의 가입 및 로그인 페이지를 호스팅하는 Amazon Cognito 사용자 지정 도메인의 도메인 접두사입니다. 사용자 지정 IdP를 사용하지 않는 경우 비워 둡니다. 그렇지 않으면 소문자, 숫자 및 하이픈만 포함해야 합니다. |

| 파라미터 | Default | 설명 |
| --- | --- | --- |
| CognitoAttributeMapping | <선택 사항 입력> | IdP 속성을 표준 및 사용자 지정 Cognito 사용자 풀 속성에 매핑합니다. 사용자 지정 IdP를 사용하지 않는 경우 비워 둡니다. 그렇지 않으면 유효한 JSON 문자열이어야 합니다. |
| IdentityType | <선택 사항 입력> | 사용할 자격 증명 공급자 유형 (`Google`, `SAML`또는 `OIDC`). 사용자 지정 IdP를 사용하지 않는 경우 비워 둡니다. |
| ProviderName | <선택 사항 입력> | 자격 증명 공급자의 이름입니다. 사용자 지정 IdP를 사용하지 않는 경우 비워 둡니다. |
| GoogleClientId | <선택 사항 입력> | 사용할 Google 클라이언트 ID입니다. IdentityType이 로 설정된 경우에만 사용되는 파라미터입니다`Google`. |
| GoogleClientSecret | <선택 사항 입력> | 사용할 Google 클라이언트 보안 암호입니다. IdentityType이 로 설정된 경우에만 사용되는 파라미터입니다`Google`. |
| SAMLMetadataURL | <선택 사항 입력> | SAML 자격 증명 공급자의 메타데이터 URL입니다. IdentityType이 SAML로 설정된 경우에만 사용되는 파라미터입니다. |
| OIDCClientId | <선택 사항 입력> | 사용할 OIDC 클라이언트 ID입니다. IdentityType이 로 설정된 경우에만 사용되는 파라미터입니다`OIDC`. |

| 파라미터 | Default | 설명 |
| --- | --- | --- |
| OIDCClientSecret | <선택 사항 입력> | 사용할 OIDC 클라이언트 보안 암호입니다. IdentityType이로 설정된 경우에만 사용되는 파라미터입니다`OIDC`. |
| OIDCIssuerURL | <선택 사항 입력> | 사용할 OIDC 발급자 URL입니다. IdentityType이 로 설정된 경우에만 사용되는 파라미터입니다`OIDC`. |
| OIDCAttributeRequestMethod | `GET` | 사용할 OIDC 속성 요청 방법입니다. `GET` 또는 중 하나여야 합니다`POST`(OIDC 공급자 참조 또는 기본값 사용). IdentityType이 로 설정된 경우에만 사용되는 파라미터입니다`OIDC`. |

6. 다음을 선택합니다.
7. Configure stack options(스택 옵션 구성) 페이지에서 Next(다음)를 선택합니다.
8. 검토 및 생성 페이지에서 설정을 검토하고 확인합니다. 템플릿이 IAM 리소스를 생성하고 특정 기능이 필요함을 확인하는 상자를 선택합니다.
9. 제출을 선택하여 스택을 배포합니다.

   AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 약 30분 후에 CREATE_COMPLETE 상태를 받게 됩니다.

> **Note**
>
> 삭제하면이 스택은 모든 리소스를 제거합니다. 스택이 업데이트되면 구성된 사용자가 손실되지 않도록 Amazon Cognito 사용자 풀이 유지됩니다.

# 배포 후 구성 작업

AWS의 워크로드 검색이 성공적으로 배포된 후 다음 배포 후 구성 작업을 완료합니다.

## Amazon Cognito에서 고급 보안 켜기

Amazon Cognito에 대한 고급 보안 기능을 활성화하려면 Amazon Cognito 개발자 안내서의 사용자 풀에 고급 보안 추가 지침을 따르세요.

> **Note**
>
> Amazon Cognito에서 고급 보안을 활성화하는 데 추가 비용이 발생합니다.

## Amazon Cognito 사용자 생성

AWS의 워크로드 검색은 Amazon Cognito를 사용하여 모든 사용자와 인증을 관리합니다. 배포 중에 사용자를 생성하고 AdminUserEmailAddress 파라미터에 제공된 주소로 임시 자격 증명과 함께 이메일을 보냅니다.

### 추가 사용자를 생성하려면:

1. AWS Cognito 콘솔에 로그인합니다.
2. 사용자 풀 관리를 선택합니다.
3. WDCognitoUserPool- *<ID-string>*을 선택합니다.
4. 탐색 창의 일반 설정에서 사용자 및 그룹을 선택합니다.
5. 사용자 탭에서 사용자 생성을 선택합니다.
6. 사용자 생성 상자에 모든 필수 필드의 값을 입력합니다.

| 양식 필드 | 필수? | 설명 |
| --- | --- | --- |
| 사용자 이름 | 예 | AWS의 워크로드 검색에 로그인하는 데 사용할 사용자 이름입니다. |

| 양식 필드 | 필수? | 설명 |
| --- | --- | --- |
| 초대장 보내기 | 예(이메일만 해당) | 선택하면가 임시 암호에 대한 알림으로 알림을 보냅니다. 이메일만 선택합니다. SMS(기본값)를 선택하면 오류 메시지가 표시되지만 사용자는 여전히 생성됩니다. |
| 임시 암호 | 예 | 임시 암호를 입력합니다. 사용자는 AWS에서 워크로드 검색에 처음 로그인할 때이 설정을 변경해야 합니다. |
| 전화번호 | 아니요 | 국제 형식으로 전화번호를 입력합니다. 예: \+44. 전화번호를 확인된 것으로 표시하시겠습니까? 상자가 선택되어 있는지 확인합니다. |
| 이메일 | 예 | 유효한 이메일 주소를 입력합니다. 이메일을 확인된 것으로 표시하시겠습니까? 상자가 선택되어 있는지 확인합니다. |

7. 사용자 생성을 선택합니다.

이 프로세스를 반복하여 필요한 수만큼 사용자를 생성합니다.

> **Note**
>
> 모든 사용자는 검색된 리소스에 대해 동일한 수준의 액세스 권한을 갖게 됩니다. 민감한 워크로드 또는 데이터가 포함된 계정에 대해 AWS에서 워크로드 검색을 별도로 배포하는 것이 좋습니다. 이렇게 하면 액세스 권한이 필요한 사용자로만 액세스를 제한할 수 있습니다.

# AWS에서 워크로드 검색에 로그인

솔루션이 성공적으로 배포된 후 솔루션의 웹 UI를 제공하는 Amazon CloudFront 배포의 URL을 확인합니다.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 중첩 보기를 선택하여 배포를 구성하는 중첩 스택을 표시합니다. 기본 설정에 따라 중첩 스택이 이미 표시될 수 있습니다.
3. AWS 스택에서 기본 워크로드 검색을 선택합니다.
4. 출력 탭을 선택하고 WebUiUrl 키와 연결된 값 열에서 URL을 선택합니다.
5. 로그인 화면에서 이메일을 통해 받은 로그인 자격 증명을 입력합니다. 그런 다음 다음 작업을 수행합니다.
   a. 프롬프트에 따라 암호를 변경합니다.
   b. 이메일로 전송된 확인 코드를 사용하여 계정 복구를 완료합니다.

# 리전 가져오기

> **Note**
> 다음 섹션은 솔루션의 계정 검색 모드가 자체 관리형인 경우에만 적용됩니다. AWS Organizations 모드에서 계정 검색이 작동하는 방식에 대한 자세한 내용은 AWS Organizations 계정 검색 모드 섹션을 참조하세요.

리전을 가져오려면 특정 인프라를 배포해야 합니다. 이 인프라는 글로벌 및 리전 리소스로 구성됩니다.

글로벌 - 계정에 한 번 배포되고 가져온 각 리전에 재사용되는 리소스입니다.

- IAM 역할(WorkloadDiscoveryRole)

리전 - 가져온 각 리전에 배포된 리소스입니다.

- AWS Config 전송 채널
- AWS Config용 Amazon S3 버킷
- IAM 역할(ConfigRole)

이 인프라를 배포하는 두 가지 옵션이 있습니다.

- AWS CloudFormation StackSets(권장)
- CloudFormation

# 리전 가져오기

이 단계에서는 리전을 가져오고 AWS CloudFormation 템플릿을 배포하는 방법을 안내합니다.

1. AWS에서 워크로드 검색에 로그인합니다. URL은 AWS에서 워크로드 검색에 로그인을 참조하세요.
2. 탐색 메뉴에서 계정을 선택합니다.
3. 가져오기를 선택합니다.
4. 가져오기 방법을 선택합니다.
   a. CSV 파일을 사용하여 계정 및 리전을 추가합니다.
   b. 양식을 사용하여 계정 및 리전을 추가합니다.

## CSV 파일

가져올 리전이 포함된 CSV(쉼표로 구분된 값) 파일을 다음 형식으로 제공합니다.

```
"accountId","accountName","region"
123456789012,"test-account-1",eu-west-2
123456789013,"test-account-2",eu-west-1
123456789013,"test-account-2",eu-west-2
123456789014,"test-account-3",eu-west-3
```

1. CSV 업로드를 선택합니다.
2. CSV 파일을 찾아 엽니다.
3. Regionstable을 검토한 다음 가져오기를 선택합니다.
4. 모달 대화 상자에서 글로벌 리소스 템플릿과 리전 리소스 템플릿을 다운로드합니다.
5. 관련 계정에 CloudFormation 템플릿을 배포합니다(AWS CloudFormation 템플릿 배포 섹션 참조).
6. 글로벌 및 리전 리소스 템플릿이 배포되면 두 상자를 모두 선택하여 설치가 완료되었는지 확인하고 가져오기를 선택합니다.

## 양식

양식을 사용하여 가져올 리전을 제공합니다.

1. 계정 ID에 12자리 계정 ID를 입력하거나 기존 계정 ID를 선택합니다.
2. 계정 이름에 계정 이름을 입력하거나 기존 계정 ID를 선택할 때 미리 채워진 값을 사용합니다.
3. 가져올 리전을 선택합니다.
4. 추가를 선택하여 아래 리전테이블의 리전을 채웁니다.
5. Regionstable을 검토한 다음 가져오기를 선택합니다.
6. 모달 대화 상자에서 글로벌 리소스 템플릿과 리전 리소스 템플릿을 다운로드합니다.
7. 관련 계정에 CloudFormation 템플릿을 배포합니다(AWS CloudFormation 템플릿 배포 섹션 참조).
8. 글로벌 및 리전 리소스 템플릿이 배포되면 두 상자를 모두 선택하여 설치가 완료되었는지 확인하고 가져오기를 선택합니다.

## AWS CloudFormation 템플릿 배포

글로벌 리소스는 계정당 한 번 배포해야 합니다. AWS의 워크로드 검색으로 이미 가져온 리전이 포함된 계정에서 리전을 가져올 때는이 템플릿을 배포하지 마십시오. 리전을 이미 가져온 경우 스택 배포의 지침에 따라 리전 리소스를 프로비저닝합니다.

## CloudFormation StackSets를 사용하여 계정 간에 글로벌 리소스 프로비저닝

> **Important**
>
> 먼저 스택 세트 작업이 대상 계정에서 StackSets를 활성화하기 위한 사전 조건을 완료합니다. StackSets

1. 관리자 계정에서 AWS CloudFormation 콘솔에 로그인합니다.
2. 탐색 메뉴에서 StackSets를 선택합니다.
3. Create StackSet(StackSet 생성)을 선택합니다.
4. 템플릿 선택 페이지의 권한에서 다음을 수행합니다.
   a. AWS Organizations를 사용하는 경우 서비스 관리형 권한 또는 셀프 서비스 권한을 선택합니다. 자세한 내용은 AWS 조직에서 StackSets 사용을 참조하세요.

b. AWS Organizations를 사용하지 않는 경우 StackSets 사전 조건 단계를 따를 때 사용되는 IAM 실행 역할 이름을 입력합니다. 자세한 내용은 자체 관리형 권한 부여를 참조하세요.

5. 템플릿 지정에서 템플릿 파일 업로드를 선택합니다. `global-resources.template` 파일을 선택하고(CSV 파일 또는 양식으로 리전을 가져올 때 이전에 다운로드됨) 다음을 선택합니다.
6. StackSet 세부 정보 지정 페이지에서 StackSet에 이름을 할당합니다. 문자 제한 이름 지정에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 및 AWS STS 할당량을 참조하세요. AWS Identity and Access Management
7. 파라미터에서이 솔루션 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

| 필드 이름 | Default | 설명 |
| --- | --- | --- |
| AccountId | 배포 계정 ID | 원래 배포 계정의 계정 ID입니다. 이 값을 기본값으로 두어야 합니다. |

1. 다음을 선택합니다.
2. StackSet 옵션 구성 페이지에서 다음을 선택합니다.
3. 배포 옵션 설정 페이지의 계정에서 계정 번호 상자에 계정 역할을 배포하기 위한 계정 IDs를 입력합니다.
4. 리전 지정에서 스택을 설치할 리전을 선택합니다.
5. 배포 옵션에서 병렬을 선택한 후 다음을 선택합니다.
6. 검토 페이지에서 AWS CloudFormation이 사용자 지정 이름으로 IAM 리소스를 생성할 수 있음을 확인하는 확인란을 선택합니다.
7. 제출을 선택합니다.

## CloudFormation StackSets를 사용하여 리전 리소스 프로비저닝

> **Important**
>
> 먼저 스택 세트 작업이 대상 계정에서 StackSets를 활성화하기 위한 사전 조건을 완료합니다. StackSets

AWS Config가 설치된 리전과 없는 리전이 있는 경우 두 개의 StackSet 작업을 수행해야 합니다. 하나는 AWS Config가 설치된 리전용이고 다른 하나는 그렇지 않은 리전용입니다.

1. 관리자 계정에서 AWS CloudFormation 콘솔에 로그인합니다.
2. 탐색 메뉴에서 StackSets를 선택합니다.
3. Create StackSet(StackSet 생성)을 선택합니다.
4. 템플릿 선택 페이지의 권한에서 다음을 수행합니다.
   a. AWS Organizations를 사용하는 경우 서비스 관리형 권한 또는 셀프 서비스 권한을 선택합니다. 자세한 내용은 AWS 조직에서 StackSets 사용을 참조하세요.
   b. AWS Organizations를 사용하지 않는 경우 StackSets 사전 조건 단계를 따를 때 사용되는 IAM 실행 역할 이름을 입력합니다. 자세한 내용은 자체 관리형 권한 부여를 참조하세요.
5. 템플릿 지정에서 템플릿 파일 업로드를 선택합니다. `regional-resources.template` 파일을 선택하고(CSV 파일 또는 양식으로 리전을 가져올 때 이전에 다운로드됨) 다음을 선택합니다.
6. StackSet 세부 정보 지정 페이지에서 StackSet에 이름을 할당합니다. 문자 제한 이름 지정에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 및 AWS STS 할당량을 참조하세요. AWS Identity and Access Management
7. 파라미터에서이 솔루션 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

| 필드 이름 | Default | 설명 |
| --- | --- | --- |
| AccountId | 배포 계정 ID | 원래 배포 계정의 계정 ID입니다. 이 값을 기본값으로 두어야 합니다. |
| AggregationRegion | 배포 리전 | 원래 배포된 리전입니다. 이 값을 기본값으로 두어야 합니다. |
| AlreadyHaveConfigSetup | No | 리전에 AWS Config가 이미 설치되어 있는지 확인합니다. AWS Config가이 리전에 이미 설치되어 있는 경우 예로 설정합니다. |

1. 다음을 선택합니다.
2. StackSet 옵션 구성 페이지에서 다음을 선택합니다.
3. 배포 옵션 설정 페이지의 계정에서 계정 번호 상자에 계정 역할을 배포할 계정 IDs를 입력합니다.
4. 리전 지정에서 스택을 설치할 리전을 선택합니다. 이렇게 하면 6단계에서 입력한 모든 계정의 이러한 리전에 스택이 설치됩니다.
5. 배포 옵션에서 병렬을 선택한 후 다음을 선택합니다.
6. 검토 페이지에서 AWS CloudFormation이 사용자 지정 이름으로 IAM 리소스를 생성할 수 있음을 확인하는 확인란을 선택합니다.
7. 제출을 선택합니다.

## CloudFormation을 사용하여 스택을 배포하여 글로벌 리소스 프로비저닝

글로벌 리소스는 계정당 한 번 배포해야 합니다. AWS의 워크로드 검색으로 이미 가져온 리전이 포함된 계정에서 리전을 가져올 때는이 템플릿을 배포하지 마십시오.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 스택 생성을 선택한 다음 새 리소스 사용(표준)을 선택합니다.
3. 스택 생성 페이지의 템플릿 지정 섹션에서 템플릿 파일 업로드를 선택합니다.
4. 파일 선택을 선택하고 (CSV `global-resources.template` 파일 또는 양식으로 리전을 가져올 때 이전에 다운로드한) 파일을 선택한 후 다음을 선택합니다.
5. 스택 세부 정보 지정 페이지에서 솔루션 스택 이름을 할당합니다. 문자 제한 이름 지정에 대한 자세한 내용은 _AWS Identity and Access Management_User Guide의 IAM 및 AWS STS 할당량을 참조하세요.
6. 파라미터에서이 솔루션 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

| 필드 이름 | Default | 설명 |
| --- | --- | --- |
| 스택 이름 | `workload-discovery` | 이 AWS CloudFormation 스택의 이름입니다. |
| AccountId | 배포 계정 ID | 원래 배포 계정의 계정 ID입니다. 이 값을 기본값으로 두어야 합니다. |

1. 다음을 선택합니다.
2. AWS CloudFormation에서 사용자 지정 이름으로 IAM 리소스를 생성할 수 있음을 확인하는 상자를 선택합니다.
3. 스택 생성을 선택합니다.

새 리전은 15:00, 15:15, 15:30, 15:45와 같이 15분 간격으로 실행되는 다음 검색 프로세스 중에 스캔됩니다.

## CloudFormation을 사용하여 스택을 배포하여 리전 리소스 프로비저닝

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 스택 생성을 선택한 다음 새 리소스 사용(표준)을 선택합니다.
3. 스택 생성 페이지의 템플릿 지정 섹션에서 템플릿 파일 업로드를 선택합니다.
4. 파일 선택을 선택하고 `regional-resources.template` 파일(CSV 파일 또는 양식으로 리전을 가져올 때 이전에 다운로드됨)을 선택한 후 다음을 선택합니다.
5. 스택 세부 정보 지정 페이지에서 솔루션 스택 이름을 할당합니다. 문자 제한 이름 지정에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 및 AWS STS 할당량을 참조하세요. AWS Identity and Access Management
6. 파라미터에서이 솔루션 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

| 필드 이름 | Default | 설명 |
| --- | --- | --- |
| AccountId | 솔루션 배포 계정 ID | 원래 배포 계정의 계정 ID입니다. 기본값으로 두어야 합니다. |
| AggregationRegion | 솔루션 배포 리전 | 원래 배포된 리전입니다. 기본값으로 두어야 합니다. |
| AlreadyHaveConfigSetup | No | 리전에 AWS Config가 이미 설치되어 있는지 확인합니다. 이 리전에 AWS Config가 이미 설치되어 있는 `Yes` 경우 로 설정합니다. |

1. 다음을 선택합니다.
2. AWS CloudFormation에서 사용자 지정 이름으로 IAM 리소스를 생성할 수 있음을 확인하는 상자를 선택합니다.
3. 스택 생성을 선택합니다.

새 리전은 15:00, 15:15, 15:30, 15:45와 같이 15분 간격으로 실행되는 다음 검색 프로세스 중에 스캔됩니다.

## 리전을 올바르게 가져왔는지 확인

1. 솔루션의 웹 UI에 로그인합니다(또는 이미 로드된 경우 페이지를 새로 고칩니다). URL은 AWS에서 워크로드 검색에 로그인을 참조하세요.
2. 왼쪽 탐색 패널의 설정에서 가져온 리전을 선택합니다.

리전, 계정 이름 및 계정 ID가 테이블에 나타납니다. 마지막으로 스캔한 열에는 해당 리전에서 마지막으로 검색된 리소스가 표시됩니다.

> **Note**
> 마지막으로 스캔한 열이 30분 이상 비워진 경우 검색 구성 요소 디버깅을 참조하세요.

# 비용 기능 설정

비용 기능을 사용하려면 AWS 비용 및 사용 보고서(CUR)를 수동으로 설정해야 합니다. 아래 지침에 따라 다음을 수행합니다.

1. 예약된 CUR을 설정합니다.
2. Amazon S3 복제 설정(CURs 배포 계정 외부에 있는 경우)

## 배포 계정에서 AWS 비용 및 사용 보고서 생성

1. 비용 데이터를 수집하려는 계정의 결제 콘솔에 로그인합니다.
2. 탐색 메뉴의 결제에서 비용 및 사용 보고서를 선택합니다.
3. 보고서 생성을 선택합니다.

4. workload-discovery-cost-and-usage- *<your-workload-discovery-deployment-account-ID>*를 보고서 이름으로 사용합니다.

> **Note**
> CURs의 쿼리를 용이하게 하기 위해 소량의 인프라가 배포되므로이 명명 규칙을 따라야 합니다.

5. 리소스 IDs 포함 상자를 선택합니다.

> **Note**
> 비용 데이터를 보려면 리소스 IDs 포함 상자를 선택해야 합니다. 이 ID는 AWS의 워크로드 검색에서 검색한 리소스와 일치해야 합니다.

6. 다음을 선택합니다.
7. 전송 옵션 페이지에서 "0" 구성을 선택합니다.
8. CUR을 저장할 *<stack-name>* -s3buc-costandusagereportbucket- *<ID-string>* Amazon S3 버킷을 선택합니다. 다음을 선택합니다.
9. 정책을 검토하고 확인 상자를 선택한 다음 저장을 선택합니다.
10. 보고서 접두사 경로를 로 설정합니다aws-perspective.
11. 시간 세부 수준을 보려면 매일을 선택합니다.
12. 에 대한 보고서 데이터 통합 활성화에서 Amazon Athena를 선택합니다.
13. 다음을 선택합니다.
14. 검토 및 완료를 선택합니다.

보고서가 올바르게 설정되었는지 확인하려면 Amazon S3 버킷에서 테스트 파일을 확인합니다.

> **Note**
> 보고서를 버킷에 업로드하는 데 최대 24시간이 걸릴 수 있습니다.

## 외부 계정에서 AWS 비용 및 사용 보고서 생성

1. 비용 데이터를 수집하려는 계정의 결제 콘솔에 로그인합니다.

2. 탐색 메뉴의 비용 관리에서 비용 및 사용 보고서를 선택합니다.
3. 보고서 생성을 선택합니다.
4. `workload-discovery-cost-and-usage-` *`<your-external-account-ID>`*를 보고서 이름으로 사용합니다.

> **Note**
> CURs의 쿼리를 용이하게 하기 위해 소량의 인프라가 배포되므로이 명명 규칙을 따라야 합니다.

5. 리소스 IDs 포함 확인란을 선택합니다.

> **Note**
> 비용 데이터를 보려면 리소스 IDs 포함 상자를 선택해야 합니다. 이 ID는 AWS의 워크로드 검색에서 검색한 리소스와 일치해야 합니다.

6. 다음을 선택합니다.
7. 전송 옵션 페이지에서 "0" 구성을 선택합니다.
8. CURs을 저장할 새 Amazon S3 버킷을 생성합니다.
9. 정책을 검토하고 확인 상자를 선택한 다음 저장을 선택합니다.
10. 보고서 접두사 경로를 로 설정합니다`aws-perspective`.
11. 시간 세부 수준을 보려면 매일을 선택합니다.
12. 에 대한 보고서 데이터 통합 활성화에서 Amazon Athena를 선택합니다.
13. 다음을 선택합니다.
14. 검토 및 완료를 선택합니다. 보고서가 올바르게 설정되었는지 확인하려면 Amazon S3 버킷에서 테스트 파일을 확인합니다.

> **Note**
> 보고서를 버킷에 업로드하는 데 최대 24시간이 걸릴 수 있습니다.

그런 다음 배포 계정에 대한 복제를 설정합니다.

# 복제 설정

배포 중에 생성된 Amazon S3 버킷으로 복제를 설정합니다. Amazon S3 버킷은 `<stack-name>-s3buc-costandusagereportbucket-<ID-string>` 형식을 따릅니다. 이렇게 하면 솔루션이 Amazon Athena로 버킷을 쿼리할 수 있습니다.

1. 복제해야 하는 생성된 CUR이 포함된 Amazon S3 콘솔의 AWS 계정에 로그인합니다.
2. CUR을 구성할 때 생성된 Amazon S3 버킷을 선택합니다. 자세한 내용은 AWS 비용 및 사용 보고서 생성 및 예약의 8단계를 참조하세요.
3. [Management] 탭을 선택한 후
4. 복제 규칙에서 복제 규칙 생성을 선택합니다.
5. 복제 규칙 구성의 복제 규칙 이름 상자에 설명이 포함된 규칙 ID를 입력합니다.
6. 소스 버킷에서 버킷의 모든 객체에 적용을 선택하여 규칙 범위를 구성합니다.
7. 대상에서 다음을 구성합니다.
   a. 다른 계정의 버킷 지정을 선택합니다.
   b. 계정 ID를 입력합니다.
   c. AWS에서 워크로드 검색을 배포하는 동안 생성된 버킷 이름의 값을 입력합니다. AWS에서 워크로드 검색을 처음 배포할 때 지정한 논리적 IDCostAndUsageReportBucket와 스택 이름을 사용하여 배포 리소스 찾기의 지침에 따라 이를 찾을 수 있습니다.
   d. 객체 소유권을 대상 버킷 소유자로 변경 확인란을 선택합니다.
8. IAM 역할에서 새 역할 생성을 선택합니다.

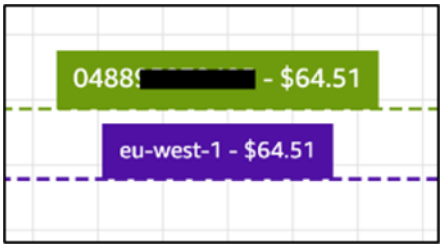
> **Note**
> 복제 역할이 이미 있을 수 있습니다. 이를 선택하고 필요한 S3 복제 역할 작업이 있는지 확인할 수 있습니다.

9. 저장을 선택합니다.
10. CUR이 설치된 AWS Management Console에 로그인하고 S3 서비스 페이지로 이동하여 CostAndUsageReportBucket S3 버킷을 선택합니다. 자세한 내용은 배포 리소스 찾기를 참조하세요.
11. 관리 탭을 선택합니다.
12. 복제 규칙의 작업 드롭다운 메뉴에서 복제된 객체 수신을 선택합니다.
13. 소스 버킷 계정 설정에서 다음을 수행합니다.

a. 소스 버킷 계정 ID를 입력합니다.
b. 정책 생성을 선택합니다.
c. 정책에서 버킷 정책 보기를 선택합니다.
d. 객체 소유권을 대상 버킷 소유자로 변경하려면 권한 포함을 선택합니다.
e. 설정 적용을 선택합니다. 이렇게 하면 객체를 복사할 수 있는 액세스 권한이 부여됩니다. 예제 S3 버킷 정책은 비용 버킷 복제 정책을 참조하세요.

> **Note**
> 여러 AWS 계정에서 CURs을 복제하는 경우. 대상 버킷의 버킷 정책(AWS 계정의 워크로드 검색 내)에 각 계정에서 사용 중인 각 IAM 역할의 ARN이 있는지 확인해야 합니다. 자세한 내용은 비용 버킷 복제 정책을 참조하세요.

보고서가 계정에 있으면 비용 데이터가 경계 상자와 개별 리소스에 표시됩니다.




# S3 버킷 수명 주기 정책 편집

배포 중에 솔루션은 두 버킷에 수명 주기 정책을 구성합니다.

- `CostAndUsageReportBucket`
- `AccessLogsBucket`

> **Important**
> 이러한 수명 주기 정책은 90일 후에 이러한 버킷에서 데이터를 삭제합니다. 보유한 모든 내부 정책에 맞게 수명 주기를 편집할 수 있습니다.

# 솔루션 모니터링

이 솔루션은 myApplications 및 CloudWatch AppInsights를 사용하여 AWS에서 워크로드 검색을 모니터링할 수 있습니다.

## myApplications

myApplications는 AWS에서 애플리케이션의 비용, 상태, 보안 태세 및 성능을 관리하고 모니터링하는 데 도움이 되는 콘솔 홈의 확장입니다. AWS Management Console의 한 보기에서 계정의 모든 애플리케이션, 모든 애플리케이션의 주요 지표, 여러 서비스 콘솔의 비용, 보안 및 운영 지표와 인사이트에 대한 개요에 액세스할 수 있습니다.

AWS에서 워크로드 검색을 위한 myApplications 대시보드를 보려면:

1. AWS Management Console에 로그인합니다.
2. 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 검색 창에 `workload-discovery`를 입력하여 애플리케이션을 찾습니다.
4. 애플리케이션을 선택합니다.

## CloudWatch AppInsights

CloudWatch Application Insights는 애플리케이션 리소스 및 기술 전반에 걸쳐 주요 지표, 로그 및 경보를 식별하고 설정하여 애플리케이션을 모니터링하는 데 도움이 됩니다. stack.It는 지표와 로그를 지속적으로 모니터링하여 이상 및 오류를 감지하고 상호 연관시킵니다. Application Insights는 문제 해결을 지원하기 위해 잠재적 근본 원인을 알려 주는 추가 인사이트와 함께 상관관계가 있는 지표 이상 및 로그 오류를 비롯하여 감지한 문제에 대한 자동화된 대시보드를 생성합니다.

AWS에서 워크로드 검색을 위한 CloudWatch AppInsights 대시보드를 보려면:

1. CloudWatch 콘솔에 로그인합니다.
2. 왼쪽 사이드바에서 Insights, Application Insights를 선택합니다.
3. 애플리케이션 탭을 선택합니다.
4. 검색 창에 `workload-discovery`를 입력하여 대시보드를 찾습니다.
5. 대시보드를 선택합니다.
6. 애플리케이션을 선택합니다.

# 솔루션 업데이트

> **Important**
>
> AWS에서 워크로드 검색의 v1.x.x에서 v2.x.x로의 업데이트는 지원되지 않습니다. v2.x.x를 설치하기 전에이 솔루션의 v1.x.x를 제거하는 것이 좋습니다.

2.x.x 배포에서 업데이트하려면 다음 단계를 따릅니다.

1. 솔루션의 AWS CloudFormation 템플릿을 다운로드합니다.
2. AWS CloudFormation 콘솔에 로그인합니다.
3. 배포 중에 제공된 이름으로 스택을 선택하고 업데이트를 선택합니다.
4. 스택 업데이트 페이지에서 현재 템플릿 교체를 선택한 다음 템플릿 파일 업로드를 선택하고 1단계에서 다운로드한 파일을 업로드합니다.
5. 다음을 선택합니다.
6. 스택 세부 정보 지정 페이지의 파라미터에서 파라미터를 검토하고 필요에 따라 수정합니다.
7. 다음을 선택합니다.
8. 스택 옵션 구성 페이지의 스택 실패 옵션에서 프로비저닝 실패 동작 라디오 버튼이 모든 스택 리소스 롤백으로 설정되어 있는지 확인합니다.
9. 다음을 선택합니다.
10. 검토 페이지에서 설정을 검토하고 확인합니다. 템플릿이 IAM 리소스를 생성하고 특정 기능이 필요함을 확인하는 상자를 선택합니다.
11. 스택 생성을 선택하여 스택을 배포합니다.

> **Note**
>
> 솔루션을 자체 관리형 계정 검색 모드로 배포한 경우 리전 가져오기 섹션의 단계에 따라 배포한 글로벌 리소스를 업데이트해야 합니다.

# 문제 해결

알려진 문제 해결은 알려진 오류를 완화하기 위한 지침을 제공합니다. 이러한 지침으로 문제가 해결되지 않는 경우 AWS 지원 문의 섹션에서이 솔루션의 AWS 지원 사례를 개설하는 방법에 대한 지침을 참조하세요.

## 알려진 문제 해결

AWS에서 워크로드 검색을 배포하는 동안과 배포 후 단계에서 다음과 같은 몇 가지 일반적인 구성 오류가 발생할 수 있습니다.

> **Note**
>
> 문제를 더 쉽게 해결할 수 있도록 AWS CloudFormation 템플릿에서 실패 시 롤백 기능을 비활성화하는 것이 좋습니다. AWS의 워크로드 검색 배포 후 구성 설명서에서 추가 문제 해결 도움말을 찾을 수도 있습니다.

### Config 전송 채널 오류

문제: 기본 AWS CloudFormation 템플릿을 배포할 때 다음 오류가 발생합니다.

```
Failed to put delivery channel '<stack-name>-DiscoveryImport-<ID-string>-
DeliveryChannel-<ID-string>' because the maximum number of delivery channels:
 1 is reached. (Service: AmazonConfig; Status Code: 400; Error Code:
 MaxNumberOfDeliveryChannelsExceededException; Request ID: 4edc54bc-8c85-4925-
b99d-7ef9c73215b3; Proxy: null)
```

이유: 솔루션이 이미 AWS Config가 활성화된 리전에 배포되고 있습니다.

해결 방법: 사전 조건 섹션의 지침에 따라 CloudFormation 파라미터 AlreadyHaveConfigSetup이 로 설정된 솔루션을 배포합니다`Yes`.

### 기존 VPC에 배포할 때 Resolver 스택 배포 시간 초과 검색

문제: OpenSearch 클러스터에서 인덱스를 생성하기 위해 사용자 지정 리소스를 프로비저닝하는 중첩 스택이 시간 초과되고 다음 오류가 발생합니다.

```
Embedded stack arn:aws:cloudformation:<region>::stack/<stack-name>-
SearchResolversStack-<ID-string>/<guid> was not successfullycreated: Stack creation
 time exceeded the specified timeout
```

이유: CloudFormation 파라미터로 제공된 프라이빗 서브넷은 S3로 라우팅할 수 없습니다(사용자 지정 리소스는 미리 서명된 URL을 사용하여 실행 결과를 S3 버킷에 작성해야 함). 여기에는 일반적으로 두 가지 이유가 있습니다.

1. 프라이빗 서브넷에는 연결된 NAT 게이트웨이가 없으므로 인터넷에 액세스할 수 없습니다.
2. 프라이빗 서브넷이 NAT 게이트웨이 대신 VPC 엔드포인트를 사용하고 있으며 S3 게이트웨이 엔드포인트가 올바르게 구성되지 않았습니다.

해결 방법:

1. VPC에서 NAT 게이트웨이를 프로비저닝하여 프라이빗 서브넷에서 실행되는 작업이 설명서에 따라 CloudFormation 또는 AWS CLI를 사용하여 인터넷에 액세스할 수 있도록 합니다.
2. 설명서에 따라 서브넷의 라우팅 테이블이 S3 VPC 엔드포인트에 대해 업데이트되었는지 확인합니다.

## 계정을 가져온 후 검색되지 않은 리소스

문제: 웹 UI를 통해 계정을 가져왔지만 검색 프로세스가 실행된 후 검색된 리소스가 없는 것으로 보입니다.

이유: 가장 가능성이 높은 이유는 다음과 같습니다.

1. CrossAccountDiscovery CloudFormation 파라미터가 로 설정된 경우 `SELF_MANAGED`글로벌 리소스 CloudFormation 템플릿이 배포되지 않은 것입니다.
2. CrossAccountDiscovery CloudFormation 파라미터가 로 설정된 경우`AWS_ORGANIZATIONS`: 하나 이상의 계정이 검색되지 않고 역할 상태 열에 배포되지 않음 항목이 있습니다. 즉, StackSets를 사용하여 글로벌 리소스 템플릿을 자동으로 배포하는 데 문제가 있었습니다.
3. 검색 프로세스 ECS 작업의 메모리가 부족합니다. 이는 많은 수의 계정 또는 리소스를 가져올 때 발생합니다. UI에서 마지막으로 검색된 열의 값은 DiscoveryTaskFrequency CloudFormation 파라미터에 지정된 값(기본값은 15분)보다 크며 ECS 콘솔에서 메모리 부족 오류가 발생합니다.

해결 방법:

1. 설명서에 따라 필요한 계정에 글로벌 리소스 템플릿을 배포합니다.
2. 워크로드 검색이 배포된 리전의 WdGlobalResources StackSet로 이동하여 배포에 실패한 스택 인스턴스의 오류를 확인합니다.
3. Memory CloudFormation 파라미터를 더 큰 값으로 업데이트합니다. 더블로 시작하고 오류가 멈출 때까지 계속 늘리세요.

> **Note**
>
> CPU 단위와 메모리 값의 특정 조합만 유효하므로 CpuUnits CloudFormation 파라미터도 업데이트해야 할 수 있습니다. 조합의 전체 목록은 ECS 설명서에 나와 있습니다.

## 특정 계정에서 AWS가 아닌 AWS Config 리소스만 검색되고 있습니다.

문제: 솔루션에서 검색하는 유일한 리소스 유형은 지원되는 리소스 섹션의 표에 나열된 리소스 유형입니다.

이유:이 문제의 가장 일반적인 원인은 다음과 같습니다.

1. CrossAccountDiscovery CloudFormation 파라미터가 로 설정된 경우 `SELF_MANAGED`리전 리소스 CloudFormation 템플릿이 검색할 각 계정의 리전에 배포되지 않은 것입니다.
2. CrossAccountDiscovery CloudFormation 파라미터를 로 설정하면 `SELF_MANAGED`리전 리소스 CloudFormation 템플릿이 Config가 활성화되지 않은 여러 계정의 리전에 배포되었지만 CloudFormation 파라미터 AlreadyHaveConfigSetup이 로 잘못 설정된 것입니다`Yes`.
3. CrossAccountDiscovery CloudFormation 파라미터를 로 설정하면 검색할 각 계정의 리전에서 `AWS_ORGANIZATIONS` AWS Config가 활성화되지 않습니다. `AWS_ORGANIZATIONS` 모드에서는 조직의 정책에 따라 Config를 활성화해야 합니다.

해결 방법:

1. 설명서에 따라 필요한 계정에 리전 리소스 템플릿을 배포합니다.
2. 이전에 배포된 리전 리소스 스택을 삭제하고(AWS Config는 일치하지 않는 상태임) CloudFormation 파라미터 AlreadyHaveConfigSetup을 로 설정하여 다시 배포합니다`No`.
3. 검색할 각 계정의 리전에서 AWS Config를 활성화합니다.

# AWS Support에 문의

AWS 개발자 지원, AWS 비즈니스 지원 또는 AWS 엔터프라이즈 지원이 있는 경우 지원 센터를 사용하여이 솔루션에 대한 전문가 지원을 받을 수 있습니다. 이후 단원에서는 그 방법에 대해서 설명합니다.

## 사례 생성

1. 지원 센터에 로그인합니다.
2. 사례 생성을 선택합니다.

## 어떻게 도와드릴까요?

1. 기술을 선택합니다.
2. 서비스에서 솔루션을 선택합니다.
3. 범주에서 기타 솔루션을 선택합니다.
4. 심각도에서 사용 사례에 가장 적합한 옵션을 선택합니다.
5. 서비스, 범주 및 심각도를 입력하면 인터페이스가 일반적인 문제 해결 질문에 대한 링크를 채웁니다. 이러한 링크로 질문을 해결할 수 없는 경우 다음 단계: 추가 정보를 선택합니다.

## 추가 정보

1. 제목에 질문 또는 문제를 요약하는 텍스트를 입력합니다.
2. 설명에서 문제를 자세히 설명합니다.
3. 파일 연결을 선택합니다.
4. AWS Support에서 요청을 처리하는 데 필요한 정보를 첨부합니다.

## 사례를 더 빠르게 해결할 수 있도록 지원

1. 요청된 정보를 입력합니다.
2. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.

## 지금 해결하거나 문의하기

1. 지금 해결 솔루션을 검토합니다.

2. 이러한 솔루션의 문제를 해결할 수 없는 경우 문의하기를 선택하고 요청된 정보를 입력한 다음 제출을 선택합니다.

# 솔루션 제거

솔루션을 제거하려면 AWS 관리 콘솔 또는 AWS 명령줄 인터페이스(AWS CLI)를 사용합니다. 먼저 Amazon ECS 클러스터에서 실행 중인 모든 작업을 중지합니다. 그렇지 않으면 스택 삭제에 실패할 수 있습니다.

## AWS 관리 콘솔 사용

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 배포 중에 제공된 이름으로 스택을 선택합니다.
3. 스택 삭제를 선택합니다.

## AWS 명령줄 인터페이스 사용

환경에서 AWS CLI를 사용할 수 있는지 확인합니다. 설치 지침은 AWS CLI 사용 설명서의AWS 명령줄 인터페이스란 무엇입니까?를 참조하세요.

AWS CLI를 사용할 수 있는지 확인한 후 다음 명령을 실행합니다.

```
$ aws cloudformation delete-stack --stack-name <customer-defined-stack-name>
```

# 개발자 안내서

이 섹션에서는 솔루션의 소스 코드와 추가 사용자 지정을 제공합니다.

## 소스 코드

AWS GitHub의 워크로드 검색 리포지토리를 방문하여이 솔루션의 템플릿 및 스크립트를 다운로드하고 사용자 지정을 다른 사용자와 공유합니다.

## 배포 리소스 찾기

다음 단계에 따라 계정에 배포된 리소스를 찾습니다.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 솔루션을 배포한 리전을 선택합니다.

   이 계정의 사용량에 따라 워크로드마다 스택이 여러 개 포함될 수 있습니다. 배포 중에 이름이 제공된 기본 스택과 그 아래에 여러 중첩 스택이 있습니다.
3. 각 스택을 선택하여 해당 템플릿을 사용하여 배포된 리소스에 액세스합니다.
4. 리소스 탭을 선택하고 관련 리소스의 물리적 ID 링크를 선택하여 해당 서비스 콘솔에서 리소스를 봅니다.

   리소스의 논리적 ID를 알고 있는 경우 테이블 위의 검색 창을 사용하여 검색할 수도 있습니다.

## 지원되는 리소스

솔루션은 여기에 나열된 대로 AWS Config가 지원하는 모든 리소스 유형을 지원합니다. 다음 표에는 AWS Config에서 지원하지 않는 AWS의 워크로드 검색에서 검색하는 지원되는 리소스가 나와 있습니다. 자세한 내용은 해당 AWS 설명서 목록에 나와 있습니다.

| 리소스 유형 | 소스 | 설명 |
| --- | --- | --- |
| AWS::APIGateway::Authorizer | SDK | getAuthorizers |
| AWS::ApiGateway::Resource | SDK | getResource |

| 리소스 유형 | 소스 | 설명 |
| --- | --- | --- |
| AWS::ApiGateway::Method | SDK | getMethod |
| AWS::Cognito::UserPool | SDK | describeUserPool |
| AWS::ECS::Task | SDK | describe-tasks |
| AWS::EKS::Nodegroup | SDK | describeNodegroup |
| AWS::DynamoDB::Stream | SDK | describeStream |
| AWS::IAM::AWSManagedPolicy | SDK | getAccountAuthorizationDetails |
| AWS::ElasticLoadBalancingV2::TargetGroup | SDK | describeTargetGroups |
| AWS::EC2::Spot | SDK | describeSpotInstanceRequests |
| AWS::EC2::SpotFleet | SDK | describeSpotFleetRequests |

## AWS Organizations 계정 검색 모드

AWS의 워크로드 검색이 AWS Organization에 배포되면 솔루션의 웹 UI를 통해 계정 검색이 더 이상 관리되지 않습니다. 이 경우 계정을 검색하기 위해 CloudFormation 템플릿 배포를 관리할 필요가 없습니다.

대신 솔루션은 AWS 조직 전체의 AWS Config 애그리게이터를 사용하여 AWS Config가 활성화된 조직의 모든 계정에서 리소스를 검색합니다.

AWS Config에서 지원하지 않는 리소스 유형의 경우 솔루션은 AWS CloudFormation StackSets. 이 역할을 통해 검색 프로세스는 조직의 모든 계정에서 SDK를 호출하여 이러한 보조 리소스를 검색할 수 있습니다.

이 StackSet는 조직에 추가된 모든 새 계정에 역할을 자동으로 배포하고 조직에서 제거된 모든 계정에서 역할을 삭제하도록 구성됩니다.

> **Note**
>
> StackSet가 관리 계정에 스택 인스턴스를 배포할 수 없습니다. 워크로드 검색에서이 계정을 검색하도록 하려면 스택 배포 섹션에 설명된 표준 AWS CloudFormation 배포 방법을 사용하여 글로벌 리소스 템플릿을 배포하여 CloudFormation을 사용하여 글로벌 리소스를 프로비저닝해야 합니다.

## Amazon S3 복제 역할 작업

복제를 수행하는 데 사용되는 IAM 역할에는 다음 작업이 있어야 합니다.

| |
|---|
| s3:ReplicateObject |
| s3:ReplicateDelete |
| s3:ReplicateTags |
| s3:ObjectOwnerOverrideToBucketOwner |
| s3:ListBucket |
| s3:GetReplicationConfiguration |
| s3:GetObjectVersionForReplication |
| s3:GetObjectVersionAcl |
| s3:GetObjectVersionTagging |
| s3:GetObjectRetention |
| s3:GetObjectLegalHold |

역할에 복제 역할 작업이 있는지 확인하려면:

1. S3 복제 마법사에서 역할 이름의 이름을 복사합니다.
2. 복제를 설정하려는 계정 내에서 IAM 콘솔에 로그인합니다.
3. 역할 이름을 IAM 검색 상자에 붙여 넣습니다.

4. 목록에서 최상위 항목을 선택합니다. 사용할 IAM 역할입니다.
5. 권한 정책에서 관리형 정책을 확장합니다.
6. 정책에 이전 표에 자세히 설명된 작업이 있는지 확인합니다.

# S3 버킷 정책

다음은 외부 계정이 객체를 복제할 수 있는 권한과 함께 CURs을 버킷에 업로드할 수 있도록 허용하는 S3 버킷 정책의 예입니다. 복제를 수행할 권한을 부여하려면 각 외부 AWS 계정의 IAM 역할을이 정책에 추가해야 합니다.

```
   {
      "Version":"2012-10-17",
      "Id":"",
      "Statement":[
          {
            "Sid":"Set permissions for objects"
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
          },
      "Action":["s3:ReplicateObject",
      "s3:ReplicateDelete"],
"s3:ObjectOwnerOverrideToBucketOwner",
        "Resource":"arn:aws:s3:::destination-bucket-name/*"
      },
      {
          "Sid":"Set permissions on bucket",
          "Effect":"Allow",
          "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
      },

      "Action":["s3:GetBucketVersioning",
"s3:PutBucketVersioning"],
        "Resource":"arn:aws:s3:::destination-bucket-name "
      },
      {
          "Sid": "Stmt1335892150622",
          "Effect": "Allow",
          "Principal": {
              "Service": "billingreports.amazonaws.com"
```

```
            },
            "Action": [
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy"
             ],
            "Resource": "arn:aws:s3:::destination-bucket-name"
        },
        {

            "Sid": "Stmt1335892526596",
            "Effect": "Allow",
            "Principal": {
                "Service": "billingreports.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::destination-bucket-name/*"

          }
      ]
    }
```

# AWS API

사전 조건에 설명된 대로 솔루션을 기존 VPC에 배포하는 경우 프라이빗 서브넷에서 다음 서비스에 액세스할 수 있어야 합니다.

## API Gateway

- GetAuthorizers
- GetIntegration
- GetMethod
- GetResources
- GetRestApis

## Cognito

- DescribeUserPool

## 구성

- BatchGetAggregateResourceConfig
- DescribeConfigurationAggregators
- ListAggregateDiscoveredResources
- SelectAggregateResourceConfig

## DynamoDB Streams

- DescribeStream

## Amazon EC2

- DescribeInstances
- DescribeSpotFleetRequests
- DescribeSpotInstanceRequests
- DescribeTransitGatewayAttachments

## Amazon Elastic Load Balancer

- DescribeLoadBalancers
- DescribeListeners
- DescribeTargetGroups
- DescribeTargetHealth

## Amazon Elastic Kubernetes 서비스

- DescribeNodegroup
- ListNodegroups

## IAM

- GetAccountAuthorizationDetails

- ListPolicies

## Lambda

- GetFunction
- GetFunctionConfiguration
- ListEventSourceMappings

## OpenSearch Service

- DescribeDomains
- ListDomainNames

## Organizations

- ListAccounts
- ListAccountsForParent
- ListOrganizationalUnitsForParent
- ListRoots

## Amazon Simple Notification Service

- ListSubscriptions

## Amazon Security Token Service

- AssumeRole

# 레퍼런스

이 섹션에는이 솔루션의 고유한 지표를 수집하기 위한 선택적 기능과이 솔루션에 기여한 빌더 목록에 대한 정보가 포함되어 있습니다.

## 익명화된 데이터 수집

이 솔루션에는 익명화된 운영 지표를 AWS로 전송하는 옵션이 포함되어 있습니다. 당사는 이 데이터를 사용하여 고객이 이 솔루션과 관련 서비스 및 제품을 어떻게 사용하는지 더 잘 이해합니다. 활성화되면 다음 정보가 수집되어 AWS로 전송됩니다.

- 솔루션 ID - AWS 솔루션 식별자
- 고유 ID(UUID) - 각 배포에 대해 무작위로 생성된 고유 식별자
- 타임스탬프 - 데이터 수집 타임스탬프
- 비용 기능 활성화됨 - 사용자가 비용 기능을 사용하고 있는지 여부에 대한 정보
- 계정 수 - 사용자가 배포에서 온보딩한 계정 수
- 다이어그램 수 - 각 배포에서 생성된 다이어그램 수
- 리소스 수 - 모든 온보딩된 계정에서 검색된 리소스 수

AWS는이 설문 조사를 통해 수집된 데이터를 소유합니다. 데이터 수집에는 개인정보 취급방침이 적용됩니다. 이 기능을 옵트아웃하려면 AWS CloudFormation 템플릿을 시작하기 전에 다음 단계를 완료하세요.

1. AWS CloudFormation 템플릿을 로컬 하드 드라이브에 다운로드합니다.
2. 텍스트 편집기를 사용하여 AWS CloudFormation 템플릿을 엽니다.
3. AWS CloudFormation 템플릿 매핑 섹션을 다음에서 수정합니다.

```
Mappings:
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'true'
```

변경 후:

```
Mappings:
```

```
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'false'
```

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 스택 생성을 선택합니다.
3. 스택 생성 페이지, 템플릿 지정 섹션에서 템플릿 파일 업로드를 선택합니다.
4. 템플릿 파일 업로드에서 파일 선택을 선택하고 로컬 드라이브에서 편집한 템플릿을 선택합니다.
5. 다음을 선택하고 스택 시작의 단계를 따릅니다.

# 기여자

- Mohsan Jaffery
- 매튜 볼
- 스테파노 보자
- Connor Kirkpatrick
- Chris Deigan
- 이닉
- 팀 메카리

# 개정

게시 날짜: 2020년 9월. 업데이트는 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.

GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.

# 고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서는 (a) 정보 제공 목적으로만 사용되며, (b) 예고 없이 변경될 수 있는 현재 AWS 제품 제공 및 관행을 나타내며, (c) AWS 및 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정 또는 보장도 생성하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 표현 또는 조건 없이 "있는 그대로" 제공됩니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

솔루션은 Apache 라이선스 버전 2.0의 약관에 따라 라이선스가 부여됩니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.