사용자 가이드

Amazon DevOps Guru

Amazon DevOps Guru: 사용자 가이드

Table of Contents

아마존 DevOps 구루란 무엇인가요?

Amazon DevOps Guru 사용 설명서에 오신 것을 환영합니다.

DevOpsGuru는 개발자와 운영자가 애플리케이션의 성능과 가용성을 쉽게 개선할 수 있는 완전 관리형 운영 서비스입니다. DevOpsGuru를 사용하면 운영 문제 식별과 관련된 관리 작업을 오프로드하여 애플리케이션 개선을 위한 권장 사항을 신속하게 구현할 수 있습니다. DevOpsGuru는 이제 애플리케이션을 개선하는 데 사용할 수 있는 사후 대응적 통찰력을 제공합니다. 또한 향후 애플리케이션에 영향을 미칠 수 있는 운영 문제를 방지하는 데 도움이 되는 사전 예방 인사이트를 제공합니다.

DevOpsGuru는 기계 학습을 적용하여 운영 데이터와 애플리케이션 지표 및 이벤트를 분석하여 정상 작동 패턴에서 벗어나는 동작을 식별합니다. DevOpsGuru가 운영 문제 또는 위험을 감지하면 알림을 받습니다. DevOpsGuru는 각 문제에 대해 현재 및 향후 예상되는 운영 문제를 해결하기 위한 지능적인 권장 사항을 제시합니다.

시작하려면 DevOpsGuru를 시작하려면 어떻게 해야 하나요?를 참조하십시오

DevOpsGuru는 어떻게 작동하나요?

DevOpsGuru 워크플로는 적용 범위와 알림을 구성할 때 시작됩니다. DevOpsGuru를 설정하면 운영 데이터 분석이 시작됩니다. 비정상적인 동작을 감지하면 문제와 관련된 지표, 로그 그룹 및 이벤트의 권장 사항 및 목록이 포함된 인사이트를 생성합니다. DevOpsGuru는 각 인사이트에 대해 알려줍니다. 활성화한 AWS Systems Manager OpsCenter 경우 Systems OpsCenter Manager를 사용하여 통찰력을 추적하고 관리할 수 있도록 OpsItem 가 생성됩니다. 각 인사이트에는 이상 동작과 관련된 권장 사항, 지표, 로그 그룹 및 이벤트가 포함됩니다. 인사이트의 정보를 사용하면 이상 행동을 이해하고 해결하는 데 도움이 됩니다.

세 가지 상위 워크플로 단계에 대한 자세한 내용은 고급 DevOps Guru 워크플로를 참조하십시오. 자세한 DevOps Guru 워크플로우다른 서비스와의 상호 작용 방식을 포함하여 DevOps Guru 워크플로에 대한 자세한 내용은 을 참조하십시오. AWS

주제

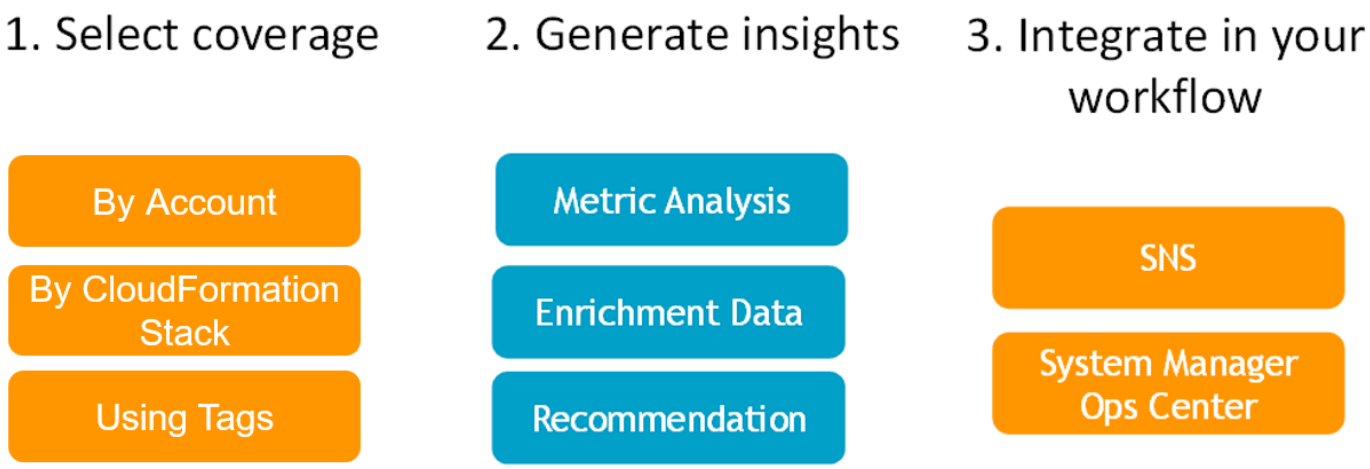
- 고급 DevOps Guru 워크플로
- 자세한 DevOps Guru 워크플로우

고급 DevOps Guru 워크플로

Amazon DevOps Guru 워크플로는 세 가지 상위 단계로 나눌 수 있습니다.

1. AWS 계정의 어떤 AWS 리소스를 분석할지 알려 DevOps Guru 적용 범위를 지정하십시오.
2. DevOpsGuru는 Amazon CloudWatch 지표 및 기타 운영 데이터를 분석하여 운영을 개선하기 위해 해결할 수 있는 문제를 식별하기 시작합니다. AWS CloudTrail
3. DevOpsGuru는 각각의 중요한 Guru 이벤트에 대한 알림을 전송하여 사용자가 통찰력과 중요한 정보에 대해 알 수 있도록 합니다. DevOps

통찰력을 추적하는 데 도움이 되는 OpsItem In을 생성하도록 DevOps AWS Systems Manager OpsCenter Guru를 구성할 수도 있습니다. 다음 다이어그램은 이 고급 워크플로를 보여 줍니다.



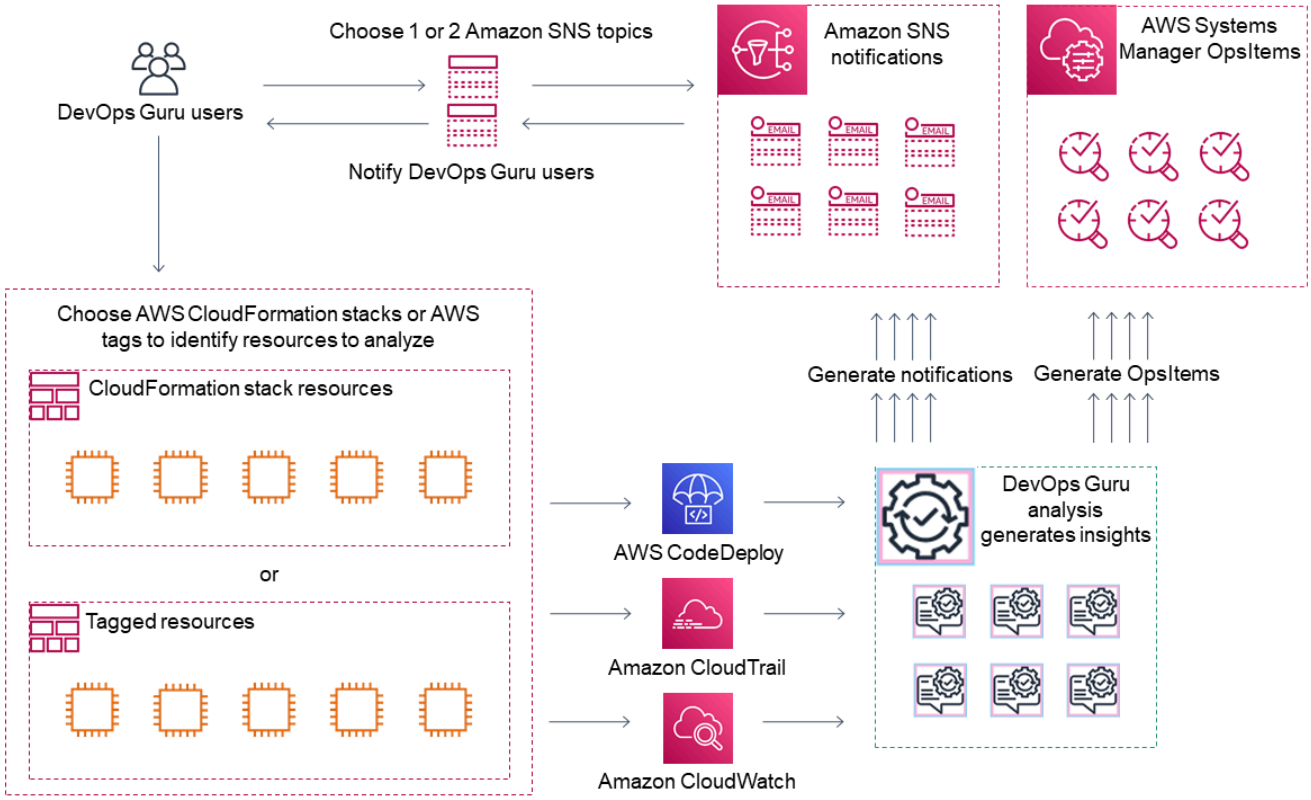
1. 첫 번째 단계에서는 분석할 AWS 계정의 AWS 리소스를 지정하여 적용 범위를 선택합니다. DevOpsGuru는 계정의 모든 리소스를 포괄하거나 분석할 수 있으며, AWS CloudFormation 스택 또는 AWS 태그를 사용하여 분석할 AWS 계정 내 리소스의 하위 집합을 지정할 수 있습니다. 지정하는 리소스가 비즈니스 크리티컬 애플리케이션, 워크로드, 마이크로서비스를 구성하는지 확인하십시오. 지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOps Guru 요금을 참조하십시오.
2. 두 번째 단계에서 DevOps Guru는 리소스를 분석하여 통찰력을 생성합니다. 진행 중인 프로세스입니다. DevOpsGuru 콘솔에서 통찰력을 보고 권장 사항 및 여기에 포함된 관련 정보를 확인할 수 있습니다. DevOpsGuru는 다음 데이터를 분석하여 문제를 찾고 통찰력을 창출합니다.
   - AWS 리소스에서 내보내는 개별 Amazon CloudWatch 지표. 문제가 식별되면 DevOps Guru는 해당 지표를 함께 수집합니다.
   - Amazon CloudWatch 로그 그룹에서 이상 징후를 기록합니다. 로그 이상 탐지를 활성화하면 문제 발생 시 DevOps Guru는 관련 로그 이상을 표시합니다.
   - DevOpsGuru는 AWS CloudTrail 관리 로그에서 보강 데이터를 가져와 수집된 지표와 관련된 이벤트를 찾습니다. 이벤트는 리소스 배포 이벤트 및 구성 변경일 수 있습니다.

- 를 사용하는 AWS CodeDeploy경우 DevOps Guru는 배포 이벤트를 분석하여 통찰력을 생성하는 데 도움이 됩니다. 모든 유형의 CodeDeploy 배포 (온프레미스 서버, Amazon EC2 서버, Lambda 또는 Amazon EC2) 에 대한 이벤트가 분석됩니다.
- DevOpsGuru는 특정 패턴을 발견하면 식별된 문제를 완화하거나 해결하는 데 도움이 되는 하나 이상의 권장 사항을 생성합니다. 권장 사항은 하나의 인사이트로 수집됩니다. 인사이트에는 문제와 관련된 지표 및 이벤트 목록도 포함됩니다. 인사이트 데이터를 사용하여 식별된 문제를 해결하고 이해합니다.

3. 세 번째 단계에서 DevOps Guru는 인사이트 알림을 워크플로우에 통합하여 문제를 관리하고 신속하게 해결할 수 있도록 지원합니다.
   - AWS 계정에서 생성된 인사이트는 Guru 설정 DevOps 중에 선택한 Amazon Simple Notification Service (Amazon SNS) 주제에 게시됩니다. 이렇게 하면 인사이트가 생성되는 즉시 알림을 받을 수 있습니다. 자세한 정보는 DevOps Guru에서 알림 업데이트을 참조하세요.
   - DevOpsGuru 설정 AWS Systems Manager 중에 활성화한 경우 각 인사이트는 발견된 문제를 추적하고 관리하는 OpsItem 데 도움이 되는 해당 정보를 생성합니다. 자세한 정보는 DevOps Guru에서 AWS Systems Manager 통합 업데이트을 참조하세요.

자세한 DevOps Guru 워크플로우

DevOpsGuru 워크플로는 Amazon CloudWatch, AWS CloudTrail Amazon 단순 알림 AWS 서비스 등을 비롯한 여러 서비스와 통합됩니다. AWS Systems Manager다음 다이어그램은 다른 AWS 서비스와의 작동 방식을 포함한 자세한 워크플로를 보여줍니다.



이 다이어그램은 AWS CloudFormation 스택에 정의된 AWS 리소스 또는 태그를 사용하여 DevOps Guru 커버리지를 지정하는 시나리오를 보여줍니다. AWS 스택이나 태그를 선택하지 않은 경우 DevOps Guru 커버리지는 계정의 모든 AWS 리소스를 분석합니다. 자세한 내용은 AWS 리소스를 사용한 애플리케이션 정의 및 DevOpsGuru에 대한 적용 범위 결정 섹션을 참조하세요.

1. 설정 중에 중요한 DevOps Guru 이벤트 (예: 인사이트 생성 시기) 에 대해 알리는 데 사용되는 Amazon SNS 주제를 하나 또는 두 개 지정합니다. 다음으로 분석하려는 리소스를 정의하는 AWS CloudFormation 스택을 지정할 수 있습니다. 또한 Systems Manager에서 각 통찰력을 생성하여 통찰력을 관리하는 데 도움이 되도록 할 수 있습니다. OpsItem
2. DevOpsGuru가 구성되면 Guru는 지표와 관련된 리소스 및 AWS CloudTrail 데이터에서 생성된 CloudWatch 지표, 로그 그룹 및 이벤트를 분석하기 시작합니다. CloudWatch 작업에 CodeDeploy 배포가 포함된 경우 DevOps Guru는 배포 이벤트도 분석합니다.

   DevOpsGuru는 분석된 데이터에서 비정상적이고 변칙적인 행동을 식별하여 통찰력을 제공합니다. 각 인사이트에는 하나 이상의 권장 사항, 인사이트를 생성하는 데 사용된 지표 목록, 관련 로그 그룹 목록, 인사이트를 생성하는 데 사용된 이벤트 목록이 포함됩니다. 이 정보를 사용하여 식별된 문제를 해결하십시오.
3. 각 인사이트가 생성되면 DevOps Guru는 Amazon SNS 주제 또는 DevOps Guru 설정 중에 지정된 주제를 사용하여 알림을 보냅니다. DevOps OpsItem Guru에서 Systems Manager를 생성하도록

설정한 경우 각 인사이트는 새 Systems OpsCenter Manager도 트리거합니다. OpsItem Systems Manager를 사용하여 통찰력을 관리할 수 OpsItems 있습니다.

DevOpsGuru를 시작하려면 어떻게 해야 하나요?

다음 단계를 수행하는 것이 좋습니다.

1. 의 정보를 읽고 DevOps Guru에 대해 자세히 알아보십시오. DevOps Guru 개념
2. 의 단계에 따라 AWS 계정 AWS CLI, 관리자 및 관리자를 설정하십시오. Amazon DevOpsGuru 설정
3. 의 지침에 따라 DevOps Guru를 사용하세요. DevOps구루와 함께 시작하기

DevOpsGuru 요금 부과를 중지하려면 어떻게 해야 하나요?

Amazon DevOps Guru를 비활성화하여 AWS 계정 및 지역의 리소스를 분석할 때 요금이 발생하지 않도록 하려면 리소스를 분석하지 않도록 적용 범위 설정을 업데이트하십시오. 이렇게 하려면 DevOps Guru에서 AWS 분석 지원 범위 업데이트의 단계를 따르고 4단계에서 None을 선택합니다. DevOpsGuru가 리소스를 분석하는 각 AWS 계정 및 지역에 대해 이 작업을 수행해야 합니다.

> **Note**
>
> 리소스 분석을 중단하도록 커버리지를 업데이트하는 경우, 과거에 DevOps Guru가 생성한 기존 인사이트를 검토하면 계속해서 소액의 요금이 부과될 수 있습니다. 이러한 요금은 인사이트 정보를 검색하고 표시하는 데 사용되는 API 호출과 관련이 있습니다. 자세한 내용은 Amazon DevOps Guru 요금을 참조하십시오.

DevOps Guru 개념

다음은 Amazon DevOps Guru의 작동 방식을 이해하는 데 필요한 중요한 개념입니다.

주제

- 이상 항목
- 인사이트
- 지표 및 운영 이벤트
- 로그 그룹 및 로그 이상 항목
- 권장 사항

이상 항목

이상 항목은 DevOps Guru에서 감지한 예상치 못하거나 비정상적인 하나 이상의 관련 지표를 나타냅니다. DevOps Guru는 기계 학습을 사용하여 AWS 리소스와 관련된 메트릭과 운영 데이터를 분석함으로써 이상 항목을 생성합니다. Amazon DevOps Guru를 설정할 때 분석할 AWS 리소스를 지정합니다. 자세한 내용은 Amazon DevOpsGuru 설정 섹션을 참조하세요.

인사이트

인사이트는 DevOps Guru를 설정할 때 지정한 AWS 리소스를 분석하는 동안 생성되는 이상 항목 모음입니다. 각 인사이트에는 운영 성과를 개선하는 데 사용할 수 있는 관찰, 권장 사항, 분석 데이터가 포함되어 있습니다. 다음과 같은 두 가지 유형의 인사이트가 있습니다.

- 사후 대응:사후 대응 인사이트는 비정상적인 동작이 발생하는 즉시 이를 식별합니다. 여기에는 현재 문제를 이해하고 해결하는 데 도움이 되는 권장 사항, 관련 지표, 이벤트와 같은 이상 항목이 포함되어 있습니다.
- 사전 예방:사전 예방 인사이트를 통해 문제가 발생하기 전에 문제를 일으킬 수 있는 행동을 파악할 수 있습니다. 여기에는 이상 항목이 문제가 발생할 것으로 예측되기 전에 문제를 해결하는 데 도움이 되는 권장 사항과 함께 포함되어 있습니다.

지표 및 운영 이벤트

인사이트를 구성하는 이상 항목은 Amazon CloudWatch에서 반환한 지표와 AWS 리소스에서 내보낸 운영 이벤트를 분석하여 생성됩니다. 애플리케이션에 있는 문제를 더 잘 이해하는 데 도움이 되는 인사이트를 생성하는 지표와 운영 이벤트를 볼 수 있습니다.

로그 그룹 및 로그 이상 항목

로그 이상 항목 감지를 활성화하면 DevOps Guru 콘솔의 DevOps Guru 인사이트 페이지에 관련 로그 그룹이 표시됩니다. 로그 그룹을 통해 리소스의 수행 및 액세스 방식에 대한 중요한 진단 정보를 알 수 있습니다.

로그 이상 항목은 로그 그룹 내에서 발견된 유사한 이상 항목 로그 이벤트의 클러스터를 나타냅니다. DevOps Guru에 표시될 수 있는 비정상적인 로그 이벤트의 예로는 키워드 이상, 형식 이상, HTTP 코드 이상 등이 있습니다.

로그 이상 항목을 사용하여 운영 문제의 근본 원인을 진단할 수 있습니다. 또한, DevOps Guru는 인사이트 권장 사항에 있는 로그 라인을 참조하여 권장되는 해결책에 대한 더 많은 컨텍스트를 제공합니다.

> **Note**
>
> DevOps Guru는 Amazon CloudWatch와 함께 작동하여 로그 이상 항목 감지를 지원합니다. 로그 이상 항목 감지를 활성화하면 DevOps Guru가 CloudWatch 로그 그룹에 태그를 추가합니다. 로그 이상 항목 감지를 끄면 DevOps Guru는 CloudWatch 로그 그룹에서 태그를 제거합니다.
> 또한, 관리자는 CloudWatch 로그를 볼 수 있는 권한이 있는 사용자만 비정상적인 CloudWatch 로그를 볼 수 있는 권한을 갖도록 해야 합니다. IAM 정책을 사용하여 `ListAnomalousLogs` 작업에 대한 액세스를 허용하거나 거부하는 것을 권장합니다. 자세한 내용은 DevOps Guru의 자격 증명 및 액세스 관리를 참조하십시오.

권장 사항

각 인사이트는 애플리케이션 성능을 개선하는 데 도움이 되는 제안 사항과 함께 권장 사항을 제공합니다. 권장 사항에는 다음과 같은 내용이 포함됩니다.

- 인사이트를 구성하는 이상 항목을 해결하기 위한 권장 사항 조치에 대한 설명.
- DevOps Guru가 비정상적인 동작을 발견한 분석된 지표 목록. 각 지표에는 메트릭과 관련된 리소스를 생성한 AWS CloudFormation 스택의 이름, 리소스 이름, 리소스와 관련된 AWS 서비스 이름이 포함됩니다.
- 인사이트와 연결된 비정상적인 지표와 관련된 이벤트 목록. 관련된 각각의 이벤트에는 이벤트와 관련된 리소스를 생성한 AWS CloudFormation 스택의 이름, 이벤트를 생성한 리소스의 이름, 이벤트와 관련된 AWS 서비스의 이름이 포함됩니다.
- 인사이트와 연결된 이상 동작과 관련된 로그 그룹 목록. 각 로그 그룹에는 샘플 로그 메시지, 보고된 로그 이상 항목 유형에 대한 정보, 로그 이상 항목이 발생한 시간, CloudWatch에서 로그 라인을 볼 수 있는 링크가 포함되어 있습니다.

DevOps전문가 취재

DevOpsGuru는 다양한 서비스를 다루고 이에 대한 통찰력을 제공합니다. AWS Guru는 DevOps Guru가 통찰력을 생성하는 각 서비스에 대해 다양한 분석된 지표와 생성된 통찰력을 표시합니다. DevOps

사후 대응 인사이트 사용 사례:

서비스 이름	사용 사례	예제	지표
AWS Lambda	콜드 스타트, 요청 증가, 다운스트림 제한 또는 코드 배포와 같은 다양한 근본적인 원인으로 인해 발생하는 Lambda 함수의 지연 시간 또는 기간 이상을 감지합니다. 신속하게 완화할 수 있는 방법을 추천합니다.	코드 배포: Amazon API Gateway 지연 시간은 최근 Lambda 코드 배포 이후 Lambda 지연 시간의 증가에 영향을 받습니다. 다운스트림 제한: 운영자가 DynamoDB의 읽기 단위 용량을 줄여 재시도 횟수가 증가했습니다. 이로 인해 제한 현상이 발생합니다. 콜드 스타트: Lambda 함수가 제대로 프로비저닝되지 않아 요청 시 Lambda가 더 오래 걸립니다.	지속 시간 제한

사전 예방 인사이트 사용 사례:

서비스 이름	사용 사례	지표
Amazon DynamoDB	DynamoDB 테이블 읽기 소비 용량이 테이블 제한에 도달할 위험이 있습니다. 권장 조치: 프로비저닝된 용량 모드를 사용하는 경우, Auto Scaling을 사용하여 테이블의 처리량 용량을 적극적으로 관리하거나 테이블의 예약 용량을 미리 구매하십시오. 온디맨드 용량 모드로 전환하여 읽기 요청당 요금을 지불하고 사용한 만큼만 요	ConsumedReadCapacityUnits

서비스 이름	사용 사례	지표
	금을 지불하십시오. 감지 시간: 6일	

서비스 적용 범위

일부 서비스의 경우 DevOps Guru는 반응형 통찰력을 제공합니다. 사후 대응 인사이트는 비정상적인 동작이 발생하는 즉시 이를 식별합니다. 여기에는 현재 문제를 이해하고 해결하는 데 도움이 되는 권장 사항, 관련 지표, 이벤트와 같은 이상 항목이 포함되어 있습니다.

일부 서비스의 경우 DevOps Guru는 사전 예방적 통찰력을 제공합니다. 사전 예방 인사이트를 통해 문제가 발생하기 전에 이상을 일으킬 수 있는 행동을 파악할 수 있습니다. 여기에는 이상 항목이 문제가 발생할 것으로 예측되기 전에 문제를 해결하는 데 도움이 되는 권장 사항과 함께 포함되어 있습니다.

DevOpsGuru는 다음과 같은 서비스에 대한 반응형 통찰력을 제공합니다.

- Amazon API Gateway
- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2

> **Note**
>
> DevOpsGuru 모니터링은 단일 인스턴스 수준이 아니라 Auto Scaling 그룹 수준에서 이루어집니다.

- Amazon ECS
- Amazon EKS
- AWS Elastic Beanstalk
- Elastic Load Balancing
- Amazon Kinesis
- AWS Lambda
- Amazon OpenSearch Service
- Amazon RDS
- Amazon Redshift

- Amazon Route 53
- Amazon S3
- Amazon SageMaker
- AWS Step Functions
- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon VPC

DevOpsGuru는 다음과 같은 서비스에 대한 사전 예방적 통찰력을 제공합니다.

- Amazon DynamoDB
- Amazon Kinesis
- AWS Lambda
- Amazon RDS
- Amazon SQS

Amazon DevOpsGuru 설정

이 섹션의 작업을 완료하여 Amazon DevOpsGuru를 처음으로 설정합니다. 이미 AWS 계정이 있고, 분석하려는 AWS 계정 또는 계정을 알고 있으며, 인사이트 알림에 사용할 Amazon Simple Notification Service 주제가 있는 경우 로 건너뛸 수 있습니다 DevOps구루와 함께 시작하기.

선택적으로 의 기능인 빠른 설정을 사용하여 DevOpsGuru AWS Systems Manager를 설정하고 옵션을 빠르게 구성할 수 있습니다. 빠른 설정을 사용하여 독립 실행형 계정 또는 조직에 DevOpsGuru를 설정할 수 있습니다. Systems Manager에서 Quick Setup을 사용하여 조직에 DevOpsGuru를 설정하려면 다음 사전 요구 사항이 있어야 합니다.

- 가 있는 조직입니다 AWS Organizations. 자세한 내용은 AWS Organizations 사용 설명서의 AWS Organizations 용어 및 개념을 참조하십시오.
- 두 개 이상의 조직 단위(OUs).
- 각 OU에서 하나 이상의 대상 AWS 계정.
- 대상 계정을 관리할 수 있는 권한이 있는 관리자 계정은 하나입니다.

빠른 설정을 사용하여 DevOpsGuru를 설정하는 방법을 알아보려면 AWS Systems Manager 사용 설명서의 빠른 설정을 사용하여 DevOpsGuru 구성을 참조하세요.

다음 단계에 따라 빠른 설정 없이 DevOpsGuru를 설정합니다.

- 1단계 - 가입 AWS
- 2단계 - DevOpsGuru에 대한 적용 범위 결정
- 3단계 - Amazon SNS 알림 주제 식별

1단계 - 가입 AWS

에 가입 AWS 계정

가 없는 경우 다음 단계를 AWS 계정완료하여 를 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/가입을 엽니다.

2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/로 이동하여 내 계정 을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 를 AWS 계정보호하고, 를 AWS 계정 루트 사용자활성화하고 AWS IAM Identity Center, 관리 사용자를 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로 에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하십시오.
2. 루트 사용자에 대해 다중 인증(MFA)을 켭니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM Identity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송URL된 로그인을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

2단계 - DevOpsGuru에 대한 적용 범위 결정

경계 범위에 따라 Amazon DevOpsGuru에서 변칙적인 동작에 대해 분석하는 AWS 리소스가 결정됩니다. 운영 애플리케이션으로 리소스를 그룹화하는 것을 권장합니다. 리소스 경계의 모든 리소스는 하나 이상의 애플리케이션을 구성해야 합니다. 운영 솔루션이 하나인 경우 범위 경계에는 해당 솔루션의 모든 리소스가 포함되어야 합니다. 애플리케이션이 여러 개인 경우 각 솔루션을 구성하는 리소스를 선택하고 AWS CloudFormation 스택 또는 AWS 태그를 사용하여 함께 그룹화합니다. 하나 이상의 애플리케이션을 정의하는지 여부에 관계없이 지정한 모든 결합된 리소스는 DevOps Guru에서 분석하고 적용 범위 경계를 구성합니다.

다음 방법 중 하나를 사용하여 운영 솔루션의 리소스를 지정합니다.

- AWS 리전 및 계정이 적용 범위 경계를 정의하도록 를 선택합니다. 이 옵션을 사용하면 DevOps Guru는 계정 및 리전의 모든 리소스를 분석합니다. 하나의 애플리케이션에만 계정을 사용하는 경우 이 옵션을 선택하는 것이 좋습니다.
- AWS CloudFormation 스택을 사용하여 운영 애플리케이션의 리소스를 정의합니다. AWS CloudFormation 템플릿은 리소스를 정의하고 생성합니다. DevOpsGuru를 구성할 때 애플리케이션 리소스를 생성하는 스택을 지정합니다. 스택은 언제든지 업데이트할 수 있습니다. 선택한 스택의 모든 리소스가 경계 범위를 정의합니다. 자세한 내용은 AWS CloudFormation 스택을 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다. 단원을 참조하십시오.

- AWS 태그를 사용하여 애플리케이션의 AWS 리소스를 지정합니다. DevOpsGuru는 선택한 태그가 포함된 리소스만 분석합니다. 이러한 리소스가 경계를 구성합니다.

  AWS 태그는 태그 키와 태그 값 으로 구성됩니다. 태그 키 하나를 지정하고 해당 키로 값을 하나 이상 지정할 수 있습니다. 애플리케이션 중 하나에서 모든 리소스에 하나의 값을 사용하십시오. 애플리케이션이 여러 개 있는 경우 모든 애플리케이션에 동일한 키가 있는 태그를 사용하고 태그의 값을 사용하여 애플리케이션에서 리소스를 그룹화하십시오. 선택한 태그가 있는 모든 리소스가 DevOpsGuru의 적용 범위 경계를 구성합니다. 자세한 내용은 태그를 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다. 단원을 참조하십시오.

경계 범위에 애플리케이션을 구성하는 리소스가 둘 이상 포함된 경우, 태그를 사용하여 애플리케이션별로 인사이트를 필터링하여 한 번에 하나씩 확인할 수 있습니다. 자세한 내용은 DevOps Guru 인사이트 보기의 4단계를 참조하십시오.

자세한 내용은 AWS 리소스를 사용한 애플리케이션 정의 단원을 참조하십시오. 지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOpsGuru 요금 섹션을 참조하세요.

3단계 - Amazon SNS 알림 주제 식별

Amazon SNS 주제를 하나 또는 두 개 사용하여 인사이트가 생성될 때와 같은 중요한 DevOpsGuru 이벤트에 대한 알림을 생성합니다. 이렇게 하면 DevOpsGuru가 가능한 한 빨리 발견하는 문제에 대해 알 수 있습니다. DevOpsGuru를 설정할 때 주제를 준비하세요. DevOpsGuru 콘솔을 사용하여 DevOpsGuru를 설정할 때 이름 또는 Amazon 리소스 이름()을 사용하여 알림 주제를 지정합니다ARN. 자세한 내용은 DevOpsGuru 활성화를 참조하세요. Amazon SNS 콘솔을 사용하여 ARN 각 주제의 및 이름을 볼 수 있습니다. 주제가 없는 경우 DevOpsGuru 콘솔을 사용하여 DevOpsGuru를 활성화할 때 주제를 생성할 수 있습니다. 자세한 내용은 Amazon Simple Notification Service 개발자 가이드의 주제 생성을 참조하십시오.

Amazon SNS 주제에 추가된 권한

Amazon SNS 주제는 AWS Identity and Access Management (IAM) 리소스 정책을 포함하는 리소스입니다. 여기에서 주제를 지정하면 DevOpsGuru는 리소스 정책에 다음 권한을 추가합니다.

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
```

```
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

DevOpsGuru가 주제를 사용하여 알림을 게시하려면 이러한 권한이 필요합니다. 해당 주제에 대해 이러한 권한을 갖고 싶지 않다면 해당 권한을 안전하게 제거할 수 있습니다. 그러면 해당 주제를 선택하기 전과 동일하게 계속 작동합니다. 그러나 이러한 추가 권한이 제거되면 DevOps구루는 주제를 사용하여 알림을 생성할 수 없습니다.

Amazon DevOps Guru 리소스 분석 비용 추정

Amazon DevOps Guru가 AWS 리소스를 분석하는 데 드는 월별 비용을 추정할 수 있습니다. 지정한 리소스 범위 내에서 각 활성 AWS 리소스에 대해 분석된 시간에 비용을 지불합니다. 리소스는 1시간 이내에 지표, 이벤트 또는 로그를 생성하는 경우에 활성화됩니다.

DevOps Guru는 선택한 리소스를 스캔하여 월별 예상 비용을 생성합니다. 리소스, 시간당 청구 가능 요금, 월별 예상 요금을 확인할 수 있습니다. 비용 예측은 기본적으로 분석된 활성 리소스가 모든 시간 동안 사용된다고 가정합니다. 예상 사용량을 기준으로 분석된 각 서비스의 비율을 변경하여 월별 예상 비용을 업데이트할 수 있습니다. 예상 비용은 리소스 분석 비용이며 DevOps Guru API 호출과 관련된 비용은 포함되지 않습니다.

한 번에 하나의 비용 예측을 생성할 수 있습니다. 예측 비용을 생성하는 데 걸리는 시간은 이를 생성할 때 지정하는 리소스 수에 따라 달라집니다. 몇 개의 리소스를 지정하는 경우, 생성을 완료하는 데 1~2시간이 걸릴 수 있습니다. 리소스를 많이 지정하는 경우, 생성을 완료하는 데 최대 4시간이 걸릴 수 있습니다. 실제 비용은 다양하며, 이는 분석된 활성 리소스를 사용한 시간의 비율에 따라 달라집니다.

> **Note**
>
> 비용 예측의 경우, 하나의 AWS CloudFormation 스택만 지정할 수 있습니다. 실제 적용 범위 경계에는 최대 1000개까지 스택을 지정할 수 있습니다.

월별 리소스 분석 비용 예측을 생성하려면

1. https://console.aws.amazon.com/devops-guru/ 에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 비용 예측기를 선택합니다.
3. DevOpsGuru를 활성화하지 않은 경우 IAM 역할을 생성해야 합니다. 나타나는 DevOpsGuru용 IAM 역할 생성 팝업 창에서 동의를 선택하여 IAM 역할을 생성합니다. 이렇게 하면 예상 DevOps 비용 분석을 시작하거나 Guru를 사용하기 시작할 때 Guru가 IAM 서비스 연결 역할을 대신 생성할 수 있습니다. DevOps 이렇게 하면 DevOps Guru는 예상 비용을 생성하는 데 필요한 권한을 갖게 됩니다. DevOpsGuru를 이미 활성화한 경우 역할은 이미 생성되었으며 이 옵션은 나타나지 않습니다.
4. 예측을 작성하는 데 사용할 리소스를 선택합니다.

   - DevOpsGuru가 하나의 AWS CloudFormation 스택으로 정의된 리소스를 분석하는 데 드는 비용을 추정하려면 다음을 수행하십시오.

1. 현재 지역의 CloudFormation 스택을 선택하세요.
2. CloudFormation 스택 선택에서 AWS 계정의 AWS CloudFormation 스택 이름을 선택합니다. 스택 이름을 입력하여 빠르게 찾을 수도 있습니다. 스택 작업 및 확인에 대한 자세한 내용은 AWS CloudFormation사용 설명서의 스택 작업을 참조하십시오.
3. (선택 사항) 현재 분석 중이 아닌 AWS CloudFormation 스택을 사용하는 경우 리소스 분석 활성화를 선택하여 DevOps Guru에서 리소스 분석을 시작할 수 있도록 하세요. DevOpsGuru를 활성화하지 않았거나 스택의 리소스를 이미 분석 중인 경우에는 이 옵션을 사용할 수 없습니다.

- DevOpsGuru가 태그를 사용하여 리소스를 분석하는 데 드는 비용을 추정하려면 다음을 수행하십시오.
  1. 현재 지역의 AWS 리소스에서 태그를 선택합니다.
  2. 태그 키에서 태그의 키를 선택합니다.
  3. 태그 값에서 (모든 값) 을 선택하거나 하나의 값을 선택합니다.
- DevOpsGuru가 AWS 계정과 지역의 리소스를 분석하는 데 드는 비용을 추정하려면 현재 지역의 AWS 계정을 선택하세요.

5. 월별 비용 예측을 선택합니다.
6. (선택 사항) 활성 리소스 사용률 % 열에 AWS 서비스에 대한 업데이트된 백분율 값을 하나 이상 입력합니다. 기본 활성 리소스 사용률 %는 100%입니다. 즉, DevOps Guru는 1시간 리소스 분석 비용을 계산한 다음, 30일 동안 총 720시간에 걸쳐 소요되는 비용을 추정하여 AWS 서비스에 대한 추정치를 산출합니다. 서비스 활성 시간이 100% 미만인 경우 예상 사용량을 기준으로 백분율을 업데이트하여 더 정확한 예상치를 얻을 수 있습니다. 예를 들어 서비스의 활성 리소스 사용률을 75%로 업데이트하면 리소스 분석에 드는 1시간 비용이 (720 x 0.75) 시간, 즉 540시간으로 추산됩니다.

예상치가 0달러인 경우 선택한 리소스에 Guru에서 지원하는 리소스가 포함되어 있지 않을 가능성이 높습니다. DevOps 지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOps Guru 요금을 참조하십시오.

DevOps구루와 함께 시작하기

이 단원에서는 Amazon DevOps Guru를 시작하여 애플리케이션의 운영 데이터 및 지표를 분석하여 통찰력을 얻는 방법을 알아봅니다.

주제

1단계: 설정

시작하기 전에 Amazon DevOpsGuru 설정에서 단계를 실행하여 준비하십시오.

2단계: Guru 활성화 DevOps

Amazon DevOps Guru를 처음 사용하도록 구성하려면 DevOps Guru를 설정하는 방법을 선택해야 합니다. 조직 전체의 애플리케이션을 모니터링하거나 현재 계정의 애플리케이션을 모니터링할 수 있습니다.

조직 전체의 애플리케이션을 모니터링하거나 현재 계정에만 DevOps Guru를 활성화할 수 있습니다. 다음 절차에서는 필요에 따라 DevOps Guru를 설정하는 다양한 방법을 설명합니다.

조직 전체의 계정을 모니터링하십시오.

조직 전체의 애플리케이션을 모니터링하기로 선택한 경우 조직 관리 계정으로 로그인하십시오. 선택 사항으로 조직 구성원 계정을 위임된 관리자로 설정할 수 있습니다. 한 번에 한 명의 위임된 관리자만 둘 수 있으며 나중에 관리자 설정을 수정할 수 있습니다. 설정한 관리 계정과 위임된 관리자 계정 모두 조직 내 모든 계정 전반에 있는 모든 인사이트에 접근할 수 있습니다.

콘솔을 사용하여 조직에 대한 교차 계정 지원을 추가하거나 AWS CLI를 사용하여 추가할 수 있습니다.

Guru 콘솔에 온보딩하세요. DevOps

콘솔을 사용하여 조직 전체의 계정에 대한 지원을 추가할 수 있습니다.

콘솔을 사용하여 DevOps Guru가 집계된 통찰력을 볼 수 있도록 하세요.

1. https://console.aws.amazon.com/devops-guru/ 에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 설정 유형으로 조직 전체의 애플리케이션 모니터링을 선택합니다.
3. 위임된 관리자로 사용하려는 계정을 선택합니다. 그리고 나서 위임된 관리자 등록을 선택합니다. 이렇게 하면 DevOps Guru를 활성화한 모든 계정의 통합 보기에 액세스할 수 있습니다. 위임된 관리자는 조직 전체의 모든 DevOps Guru 인사이트와 지표를 통합적으로 볼 수 있습니다. SSM 빠른 설정 또는 AWS CloudFormation 스택 세트를 사용하여 다른 계정을 활성화할 수 있습니다. 빠른 설정에 대해 자세히 알아보려면 빠른 설정으로 DevOps Guru 구성을 참조하십시오. 스택 세트를 사용하여 설정하는 방법에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 스택 활용하기, 2단계 - DevOpsGuru에 대한 적용 범위 결정 및 AWS CloudFormation 스택을 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다.을 참고하십시오.

AWS CLI를 통한 온보딩

AWS CLI를 사용하여 DevOps Guru가 집계된 통찰력을 볼 수 있도록 할 수 있습니다. 다음 명령을 실행합니다.

```
aws iam create-service-linked-role --aws-service-name devops-guru.amazonaws.com --
description "My service-linked role to support DevOps Guru"

aws organizations enable-aws-service-access --service-principal devops-
guru.amazonaws.com

aws organizations register-delegated-administrator --account-id >ACCOUNT_ID< --service-
principal devops-guru.amazonaws.com
```

다음 표는 명령을 설명합니다.

Command	설명
`create-service-linked-role`	DevOpsGuru에게 조직에 대한 정보를 수집할 수 있는 권한을 부여합니다. 이 단계가 성공적으로 완료되지 않으면 진행하지 마십시오.
`enable-aws-service-access`	조직을 Guru에 온보딩하십시오. DevOps

Command	설명
`register-delegated-administrator`	구성원 계정에 액세스할 수 있는 권한을 부여하여 인사이트를 확인합니다.

현재 계정 모니터링

현재 계정에서 애플리케이션을 모니터링하기로 선택한 경우, AWS 계정 및 지역에서 다루거나 분석할 AWS 리소스를 선택하고 인사이트가 생성될 때 알려주는 데 사용되는 Amazon Simple Notification Service 주제를 한두 개 지정하십시오. 이 설정은 필요에 따라 나중에 업데이트할 수 있습니다.

DevOpsGuru가 현재 AWS 계정의 애플리케이션을 모니터링할 수 있도록 지원하세요.

1. https://console.aws.amazon.com/devops-guru/ 에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 설정 유형으로 현재 AWS 계정의 애플리케이션 모니터링을 선택합니다.
3. DevOpsGuru 분석 커버리지에서 다음 중 하나를 선택하십시오.
   - 현재 AWS 계정의 모든 AWS 리소스 분석: DevOps Guru는 계정의 모든 AWS 리소스를 분석합니다.
   - 분석할 AWS 리소스 나중에 선택: 분석 경계를 나중에 선택합니다. 자세한 내용은 DevOpsGuru에 대한 적용 범위 결정 및 DevOps Guru에서 AWS 분석 지원 범위 업데이트 섹션을 참조하세요.

   DevOpsGuru는 지원하는 AWS 계정과 관련된 모든 리소스를 분석할 수 있습니다. 지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOps Guru 요금을 참조하십시오.
4. 주제를 두 개까지 추가할 수 있습니다. DevOpsGuru는 주제 또는 주제를 사용하여 새로운 통찰력 생성과 같은 중요한 DevOps Guru 이벤트에 대해 알려줍니다. 지금 주제를 지정하지 않으면 탐색 창에서 설정을 선택하여 나중에 추가할 수 있습니다.
   a. Amazon SNS 주제 지정에서 사용할 주제를 선택합니다.
   b. Amazon SNS 주제를 추가하려면 다음 중 하나를 수행합니다.
      - 이메일을 사용하여 새 SNS 주제 생성을 선택합니다. 그런 후에 이메일 주소 지정에서 알림을 받으려는 이메일 주소를 입력합니다. 추가 이메일 주소를 입력하려면 새 이메일 추가를 선택합니다.

- 기존 SNS 주제 사용을 선택합니다. 그런 다음 AWS 계정의 주제 선택에서 사용하려는 주제를 선택합니다.
- 기존의 SNS 주제 ARN을 선택하여 다른 계정의 기존 주제 지정을 선택합니다. 그런 후에 주제의 ARN 입력에서 주제 ARN을 입력합니다. ARN은 주제에 대한 Amazon 리소스 이름(ARN)입니다. 다른 계정에서 주제를 지정할 수도 있습니다. 다른 계정에서 주제를 사용하는 경우 주제에 리소스 정책을 추가해야 합니다. 자세한 내용은 Amazon SNS 주제에 대한 권한 섹션을 참조하십시오.

5. 활성화를 선택합니다.

Amazon DevOps Guru를 처음 사용하도록 구성하려면 계정 및 지역에서 다루거나 분석할 AWS 리소스를 선택하고, 인사이트가 생성될 때 알려주는 데 사용되는 Amazon Simple Notification Service 주제를 하나 또는 두 개 지정해야 합니다. 이 설정은 필요에 따라 나중에 업데이트할 수 있습니다.

3단계: DevOps Guru 리소스 커버리지를 지정하십시오.

나중에 DevOps Guru를 활성화했을 때 AWS 리소스를 지정하기로 선택한 경우 분석하려는 리소스를 생성하는 AWS 계정의 AWS CloudFormation 스택을 선택해야 합니다. AWS CloudFormation 스택은 단일 단위로 관리하는 AWS 리소스 모음입니다. 하나 이상의 스택을 사용하여 운영 애플리케이션을 실행하는 데 필요한 모든 리소스를 포함한 다음 DevOps Guru에서 분석하도록 지정할 수 있습니다. 스택을 지정하지 않으면 DevOps Guru는 계정의 모든 AWS 리소스를 분석합니다. 자세한 내용은 AWS CloudFormation 사용자 가이드의 스택으로 작업하기 및DevOpsGuru에 대한 적용 범위 결정, AWS CloudFormation 스택을 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다.를 참조하십시오.

> **Note**
>
> 지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOps Guru 요금을 참조하십시오.

DevOpsGuru 리소스 커버리지를 지정하십시오.

1. https://console.aws.amazon.com/devops-guru/ 에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 분석된 리소스에서 분석된 리소스 편집을 선택합니다.
4. 다음 커버리지 옵션 중 하나를 선택합니다.

- DevOpsGuru가 계정 및 지역에서 지원되는 모든 리소스를 분석하도록 하려면 모든 AWS 계정 리소스를 선택합니다. 이 옵션을 선택하면 AWS 계정이 리소스 분석 적용 범위 범위가 됩니다. 계정의 각 스택에 있는 모든 리소스는 자체 애플리케이션으로 그룹화됩니다. 스택에 없는 나머지 리소스는 모두 자체 애플리케이션으로 그룹화됩니다.
- 선택한 CloudFormation 스택에 있는 리소스를 DevOps Guru가 분석하도록 하려면 스택을 선택하고 다음 옵션 중 하나를 선택하십시오.
  - 모든 리소스 - 계정의 스택에 있는 모든 리소스가 분석됩니다. 각 스택의 리소스는 자체 애플리케이션으로 그룹화됩니다. 스택에 없는 계정 내 리소스는 분석되지 않습니다.
  - 스택 선택 — Guru가 분석할 스택을 선택합니다. DevOps 선택한 각 스택의 리소스는 자체 애플리케이션으로 그룹화됩니다. 스택 찾기에서 스택 이름을 입력하여 특정 스택을 빠르게 찾을 수 있습니다. 최대 1,000개의 스택을 선택할 수 있습니다.

  자세한 정보는 AWS CloudFormation 스택을 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다.을 참조하세요.
- 선택한 태그가 포함된 모든 리소스를 DevOps Guru가 분석하도록 하려면 태그를 선택하세요. 키를 선택하고, 다음 옵션 중 하나를 선택합니다.
  - 모든 계정 리소스 - 현재 리전 및 계정의 모든 AWS 리소스를 분석합니다. 선택한 태그 키가 있는 리소스는 태그 값이 있는 경우 그 값을 기준으로 그룹화됩니다. 이 태그 키가 없는 리소스는 별도로 그룹화되고 분석됩니다.
  - 특정 태그 값 선택 - 선택한 키의 태그가 포함된 모든 리소스가 분석됩니다. DevOpsGuru는 태그 값에 따라 리소스를 애플리케이션으로 그룹화합니다.

  이 태그의 키는 `devops-guru-` 접두사로 시작해야 합니다. 이 프리픽스는 대소문자를 구분하지 않습니다. 예를 들어, 유효한 키는 `DevOps-Guru-Production-Applications`입니다. 자세한 정보는 태그를 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다.을 참조하세요.
- DevOpsGuru가 리소스를 분석하지 못하게 하려면 없음을 선택하세요. 이 옵션은 DevOps Guru를 비활성화하여 리소스 분석으로 인한 요금 발생을 중단합니다.

5. 저장을 선택합니다.

DevOps Guru 분석을 위한 AWS 서비스 활성화

Amazon DevOps Guru는 지원하는 모든 AWS 리소스의 성능을 분석할 수 있습니다. 비정상적인 동작을 발견하면 해당 동작에 대한 세부 정보와 이를 해결하는 방법을 포함한 인사이트를 생성합니다. 지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOps Guru 요금을 참고하십시오.

DevOps Guru는 Amazon CloudWatch 지표, AWS CloudTrail 이벤트 등을 사용하여 리소스를 분석하는 데 도움을 줍니다. 지원하는 대부분의 리소스는 DevOps Guru 분석에 필요한 지표를 자동으로 생성합니다. 하지만 일부 AWS 서비스에서는 필요한 지표를 생성하기 위한 추가 조치가 필요합니다. 일부 서비스의 경우 이러한 지표를 활성화하면 기존 DevOps Guru 범위에 대한 추가 분석이 제공됩니다. 다른 경우에는 이러한 지표를 활성화할 때까지 분석이 불가능합니다. 자세한 정보는 DevOpsGuru에 대한 적용 범위 결정 및 DevOps Guru에서 AWS 분석 지원 범위 업데이트 섹션을 참조하세요.

DevOps Guru 분석을 위한 조치가 필요한 서비스

- Amazon Elastic Container Service — DevOps Guru의 리소스 적용 범위를 개선하는 추가 지표를 생성하려면 Amazon ECS에서 컨테이너 인사이트 설정의 단계를 따르십시오. 이렇게 하면 Amazon CloudWatch 요금이 부과될 수 있습니다.
- Amazon Elastic Kubernetes Service — DevOps Guru가 분석할 지표를 생성하려면 Amazon EKS 및 Kubernetes에서 컨테이너 인사이트 설정의 단계를 따르십시오. 이러한 지표를 생성하기 전까지 DevOps Guru는 Amazon EKS 리소스를 분석하지 않습니다. 이렇게 하면 Amazon CloudWatch 요금이 부과될 수 있습니다.
- Amazon Simple Storage Service — DevOps Guru가 분석할 지표를 생성하려면 요청 지표를 활성화해야 합니다. 버킷의 모든 객체에 대한 CloudWatch 지표 구성 생성의 단계를 따르십시오. 이러한 지표가 생성되기 전까지 DevOps Guru는 Amazon S3 리소스를 분석하지 않습니다. 이렇게 하면 CloudWatch 및 Amazon S3 요금이 부과될 수 있습니다.

자세한 내용은 Amazon CloudWatch 요금을 참조하세요.

DevOps Guru에서 인사이트 활용

Amazon DevOps Guru는 운영 애플리케이션에서 비정상적인 동작을 감지하면 인사이트를 생성합니다. DevOps Guru는 DevOps Guru를 설정할 때 지정한 AWS 리소스에 있는 지표, 이벤트 등을 분석합니다. 각 인사이트에는 문제를 완화하기 위해 취해야 할 권장 사항이 하나 이상 포함되어 있습니다. 또한, 지표 목록, 로그 그룹 목록, 비정상적인 동작을 식별하는 데 사용된 이벤트 목록도 포함되어 있습니다.

인사이트 유형은 두 가지가 있습니다.

- 사후 대응형 인사이트에는 현재 발생하고 있는 문제를 해결하기 위해 취할 수 있는 권장 사항이 있습니다.
- 사전 예방형 인사이트에는 DevOps Guru가 앞으로 발생할 것으로 예측하는 문제를 해결하는 권장 사항이 있습니다.

주제

DevOps Guru 인사이트 보기

AWS Management Console을(를) 사용하여 인사이트를 확인할 수 있습니다.

DevOps Guru 인사이트 보기

1. https://console.aws.amazon.com/devops-guru/에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 사후 대응형 탭에서는 사후 대응형 인사이트 목록을 볼 수 있습니다. 사전 예방형 탭에서는 사전 예방형 인사이트 목록을 볼 수 있습니다.
4. (선택 사항) 다음 필터 중 하나 이상을 사용하여 원하는 인사이트를 찾습니다.
    - 찾고 있는 인사이트 유형에 따라 사후 대응형 또는 사전 예방형 탭을 선택하십시오.

- 필터 인사이트 선택한 다음, 필터를 지정하는 옵션을 선택합니다. 상태, 심각도, 리소스, 태그 필터 조합을 추가할 수 있습니다. AWS 태그 필터를 사용하면 특정 태그가 있는 리소스에서만 생성된 인사이트를 볼 수 있습니다. 자세한 내용은 태그를 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다. 단원을 참조하십시오.

> **Note**
>
> DevOps Guru는 다음과 같은 리소스를 분석할 수 있지만, 태그를 사용하여 인사이트를 필터링할 수는 없습니다.
>
> - Amazon API Gateway 경로 및 경로
> - Amazon DynamoDB Streams
> - Amazon EC2 Auto Scaling 그룹 인스턴스
> - AWS Elastic Beanstalk 환경
> - Amazon Redshift 노드

- 인사이트 생성 시간을 기준으로 필터링할 시간 범위를 선택하거나 지정합니다.
  - 12h는 지난 12시간 동안 생성된 인사이트를 보여줍니다.
  - 1d는 지난 하루 동안 생성된 인사이트를 보여줍니다.
  - 1w는 지난 한 주 동안 생성된 인사이트를 보여줍니다.
  - 1m는 지난 한 달 동안 생성된 인사이트를 보여줍니다.
  - 사용자 지정을 사용하면 또 다른 시간 범위를 지정할 수 있습니다. 인사이트를 필터링하는 데 사용할 수 있는 최대 시간 범위는 180일입니다.

5. 인사이트에 대한 세부 정보를 보려면 해당 이름을 선택합니다.

DevOps Guru 콘솔에서 인사이트 이해하기

Amazon DevOps Guru 콘솔을 사용하면 인사이트에 있는 유용한 정보를 확인하여 이상 동작을 진단하고 해결하는 데 도움이 됩니다. DevOps Guru는 리소스를 분석하고 비정상적인 동작을 나타내는 관련된 Amazon CloudWatch 지표, AWS CloudTrail 이벤트 및 운영 데이터를 찾으면 문제를 해결하기 위한 권장 사항과 관련 지표 및 이벤트에 대한 정보가 포함된 인사이트를 생성합니다. DevOps Guru 모범 사례와(과) 함께 인사이트 데이터를 사용하여 DevOps Guru에서 감지한 운영 문제를 해결합니다.

인사이트를 보려면 인사이트 보기에서 다음 단계에 따라 인사이트를 찾은 다음, 해당 이름을 선택합니다. 인사이트 페이지에는 다음 정보가 포함되어 있습니다.

인사이트 개요

이 섹션에서는 인사이트의 개괄적인 개요를 살펴봅니다. 인사이트 상태(진행 중 또는 종료됨), 영향을 받는 AWS CloudFormation 스택 수, 인사이트 시작, 종료 및 최종 업데이트 시기, 관련 작업 항목이 있는 경우 해당 항목을 확인할 수 있습니다.

인사이트가 스택 수준에서 그룹화된 경우 영향을 받는 스택의 수를 선택하여 이름을 볼 수 있습니다. 인사이트를 생성한 이상 동작은 영향을 받은 스택에서 생성된 리소스에서 발생했습니다. 인사이트가 계정 수준에서 그룹화되면 숫자가 0이거나 나타나지 않습니다.

자세한 내용은 이상 동작이 인사이트로 그룹화되는 방식 이해하기 섹션을 참조하세요.

인사이트 이름

인사이트 이름은 스택 수준에서 그룹화되는지 아니면 계정 수준에서 그룹화되는지에 따라 달라집니다.

- 스택 수준 인사이트 이름에는 비정상적인 동작이 있는 리소스가 포함된 스택의 이름이 포함됩니다.
- 계정 수준 인사이트 이름에는 스택 이름이 포함되지 않습니다.

자세한 내용은 이상 동작이 인사이트로 그룹화되는 방식 이해하기 섹션을 참조하세요.

집계된 측정치

집계된 지표 탭을 선택하면 인사이트와 관련된 지표를 볼 수 있습니다. 표에서 각 행은 지표 하나를 나타냅니다. 지표를 내보낸 리소스를 생성한 AWS CloudFormation 스택이 어느 스택인지, 리소스 이름 및 유형을 확인할 수 있습니다. 모든 지표가 AWS CloudFormation 스택과 연결되거나 이름이 있는 것은 아닙니다.

이상 리소스가 동시에 여러 개 있는 경우 타임라인 뷰가 리소스를 집계하고 이상 지표를 하나의 타임라인에 표시하여 쉽게 분석할 수 있도록 합니다. 타임라인의 빨간색 선은 지표에서 비정상적인 값이 나온 시간 범위를 나타냅니다. 확대하려면 마우스를 사용하여 특정 시간 범위를 선택합니다. 돋보기 아이콘을 사용하여 확대 및 축소할 수도 있습니다.

타임라인에서 빨간색 선을 선택하면 자세한 정보를 볼 수 있습니다. 열리는 창에서 다음과 같은 내용을 수행할 수 있습니다.

- CloudWatch 콘솔에서 지표가 어떻게 보이는지 확인하려면 CloudWatch에서 보기를 선택합니다. 자세한 정보는 Amazon CloudWatch 사용 설명서의 통계 및 규모를 참조하세요.

- 그래프 위에 마우스를 올려 놓으면 이상 지표 데이터와 발생 시기에 대한 세부 정보를 볼 수 있습니다.
- 그래프의 PNG 이미지를 다운로드하려면 아래쪽 화살표가 있는 상자를 선택합니다.

그래프로 표시된 이상 항목

그래프로 표시된 이상 항목 탭을 선택하면 인사이트의 이상 현상 각각에 대해 자세한 그래프를 볼 수 있습니다. 각각의 이상 항목에 대해 관련 지표에서 감지된 비정상적인 동작에 대한 세부 정보가 포함된 타일 하나가 표시됩니다. 리소스 수준 및 통계별로 이상 항목을 조사하고 살펴볼 수 있습니다. 그래프는 지표 이름을 기준으로 그룹화됩니다. 각 타일에서 타임라인의 특정 시간 범위를 선택하여 확대할 수 있습니다. 돋보기 아이콘을 사용하여 확대 및 축소하거나 시간, 일 또는 주 단위로 미리 정의된 기간(1H, 3H, 12H, 1D, 3D, 1W, 2W)을 선택할 수도 있습니다.

모든 통계 및 차원 보기를 선택하면 이상 항목에 대한 세부 정보를 볼 수 있습니다. 열리는 창에서 다음과 같은 내용을 수행할 수 있습니다.

- CloudWatch 콘솔에서 지표가 어떻게 보이는지 확인하려면 CloudWatch에서 보기를 선택합니다.
- 그래프 위에 마우스를 올려 놓으면 이상 지표 데이터와 발생 시기에 대한 세부 정보를 볼 수 있습니다.
- 통계 또는 차원을 선택하여 그래프의 표시 내용을 사용자 지정합니다. 자세한 정보는 Amazon CloudWatch 사용 설명서의 통계 및 규모를 참조하세요.

로그 그룹

로그 이상 항목 감지를 활성화하면 DevOps Guru가 CloudWatch 로그 그룹에 태그를 지정하므로 인사이트와 관련된 로그 그룹을 볼 수 있습니다. 인사이트 세부 정보 페이지의 로그 그룹 섹션에서 표의 각 행은 하나의 로그 그룹을 나타내며 관련 리소스를 나열합니다.

여러 개의 이상 로그 그룹이 동시에 있는 경우 타임라인 뷰가 이를 집계하여 하나의 타임라인으로 표시하므로 쉽게 분석할 수 있습니다. 타임라인의 보라색 선은 로그 그룹에서 로그 이상 항목이 발생한 시간 범위를 나타냅니다.

타임라인에서 보라색 선을 선택하면 키워드 예외 및 수치 편차와 같은 로그 이상 항목 정보에 대한 샘플을 볼 수 있습니다. 로그 이상 항목을 보려면 로그 그룹 세부 정보 보기를 선택합니다. 열리는 창에서 다음과 같은 내용을 수행할 수 있습니다.

- 로그 이상 현상 및 관련 이벤트의 그래프를 볼 수 있습니다.
- 그래프 위에 커서를 올리면 이상 로그 데이터 및 발생 시기에 대한 세부 정보를 볼 수 있습니다.
- 샘플 메시지, 발생 빈도, 관련 권장 사항, 발생 시간과 함께 로그 이상 항목을 자세히 볼 수 있습니다.

- CloudWatch에서 세부 정보 보기를 클릭하면 로그 이상 항목의 로그 라인을 볼 수 있습니다.

관련 이벤트

관련 이벤트에서 인사이트와 관련된 AWS CloudTrail 이벤트를 확인할 수 있습니다. 이러한 이벤트를 사용하면 이상 동작의 근본 원인을 이해, 진단, 해결하는 데 도움이 됩니다.

권장 사항

권장 사항에서 근본적인 문제를 해결하는 데 도움이 될 수 있는 제안 사항을 확인할 수 있습니다. DevOps Guru는 비정상적인 동작을 감지하면 권장 사항을 만드는 시도를 합니다. 인사이트에는 권장 사항이 하나, 여러 개 또는 0개가 있을 수 있습니다.

이상 동작이 인사이트로 그룹화되는 방식 이해하기

인사이트는 스택 수준 또는 계정 수준에서 그룹화됩니다. AWS CloudFormation 스택에 있는 리소스에 대해 생성된 인사이트의 경우, 이 인사이트는 스택 수준 인사이트입니다. 그렇지 않은 경우에는 계정 수준 인사이트입니다.

스택을 그룹화하는 방법은 귀하가 Amazon DevOps Guru에서 리소스 분석 범위를 구성한 방법에 따라 달라질 수 있습니다.

범위가 AWS CloudFormation 스택 기준으로 정의한 경우

선택한 스택에 포함된 모든 리소스가 분석되고 감지된 모든 인사이트는 스택 수준에서 그룹화됩니다.

범위가 귀하의 현재 AWS 계정 및 지역인 경우

귀하의 계정 및 지역에 있는 모든 리소스가 분석되며, 감지된 인사이트에 대해 그룹화가 가능한 시나리오가 세 개 있습니다.

- 스택에 속하지 않는 리소스에서 생성된 인사이트는 계정 수준에서 그룹화됩니다.
- 맨 처음 10,000개의 분석된 스택 중 하나에 있는 리소스에서 생성된 인사이트는 스택 수준에서 그룹화됩니다.
- 맨 처음 10,000개의 분석된 스택에 속하지 않는 리소스에서 생성된 인사이트는 계정 수준에서 그룹화됩니다. 예를 들어, 10,001번째로 분석된 스택에 있는 리소스에 대해 생성된 인사이트는 계정 수준에서 그룹화됩니다.

자세한 내용은 DevOpsGuru에 대한 적용 범위 결정 섹션을 참조하세요.

인사이트 심각도 이해

인사이트는 높음, 중간, 낮음이라는 세 가지 심각도 중 하나를 가질 수 있습니다. Amazon DevOps Guru는 관련된 이상 항목을 감지하고 각 이상 항목에 심각도를 할당한 후 인사이트를 생성합니다. DevOps Guru는 도메인 지식과 다년간의 집단적 경험을 사용하여 이상 항목에 심각도를 높음, 중간 또는 낮음으로 할당합니다. 인사이트의 심각도는 인사이트 생성에 기여한 가장 심각한 이상 항목에 의해 결정됩니다.

- 인사이트를 생성한 모든 이상 항목의 심각도가 낮음이면 인사이트의 심각도는 낮음입니다.
- 인사이트를 생성한 모든 이상 항목 중 가장 높은 심각도가 중간이면 인사이트의 심각도는 중간입니다. 인사이트를 생성한 이상 항목 중 일부의 심각도는 낮음일 수 있습니다.
- 인사이트를 생성한 모든 이상 항목 중 가장 높은 심각도가 높음이면 인사이트의 심각도는 높음입니다. 인사이트를 생성한 이상 항목 중 일부의 심각도는 낮음이거나 중간일 수 있습니다.

DevOpsGuru를 사용한 데이터베이스 모니터링

DevOpsGuru는 데이터베이스 운영에 상당한 가치를 제공합니다. AWS DevOpsGuru는 기계 학습 알고리즘을 활용하여 데이터베이스 성능을 최적화하고 안정성을 개선하며 운영 오버헤드를 줄이는 데 도움을 줄 수 있습니다. 사용자 가이드의 이 섹션에서는 다양한 데이터베이스 서비스에 대한 특정 DevOps Guru 사용 사례를 포함하여 이러한 데이터베이스 기능에 대한 높은 수준의 개요를 제공합니다. AWS

DevOpsGuru는 Amazon RDS 및 와 같은 관계형 데이터베이스에 대한 통찰력을 제공할 수 있습니다. Amazon Redshift 또한 및 와 같은 비관계형 또는 NoSQL 데이터베이스에 대한 통찰력을 제공할 수 있습니다. Amazon DynamoDB Amazon ElastiCache

주제

- Guru를 사용하여 관계형 데이터베이스를 모니터링합니다. DevOps
- Guru를 사용한 비관계형 데이터베이스 모니터링 DevOps

Guru를 사용하여 관계형 데이터베이스를 모니터링합니다. DevOps

DevOpsGuru는 두 개의 기본 데이터 소스에서 데이터를 가져와 관계형 데이터베이스에서 인사이트와 이상 징후를 찾습니다. Amazon RDS 및 의 Amazon Redshift 경우 CloudWatch 벤드 메트릭은 모든 인스턴스 유형에 대해 분석됩니다. Amazon RDS의 경우 Performance Insights 데이터는 PostgreSQL용 RDS, Aurora PostgreSQL 및 Aurora MySQL과 같은 엔진 유형에 대해서도 수집됩니다.

Amazon RDS에서의 데이터베이스 작업 모니터링

이 섹션에는 표준 지표 및 Performance Insights의 데이터를 포함하여 DevOps Guru for RDS에서 CloudWatch 모니터링되는 사용 사례 및 지표에 대한 구체적인 정보가 포함되어 있습니다. 주요 개념, 구성 및 이점을 비롯한 DevOps Guru for RDS에 대한 자세한 내용은 을 참조하십시오. the section called “RDS용 Guru에서 예외 항목 다루기 DevOps”

표준 지표의 데이터를 사용하여 RDS를 모니터링합니다. CloudWatch

DevOpsGuru는 CPU 사용률, 읽기 및 쓰기 작업 지연 시간과 같은 기본 CloudWatch 메트릭을 수집하여 모든 유형의 RDS 인스턴스를 모니터링할 수 있습니다. 이러한 지표는 기본적으로 제공되므로 DevOps Guru로 RDS 인스턴스를 모니터링할 때 추가 구성을 하지 않아도 통찰력을 얻을 수 있습니다. DevOpsGuru는 기록 패턴을 기반으로 이러한 지표의 기준을 자동으로 설정하고 이를 실시간 데이터와 비교하여 데이터베이스의 이상 현상과 잠재적 문제를 탐지합니다.

다음 표에는 CloudWatch 벤더 메트릭에서 Amazon RDS에 대한 잠재적 반응형 인사이트 목록이 나와 있습니다.

AWS Guru가 모니터링한 리소스 DevOps	DevOps구루가 식별한 시나리오	CloudWatch 지표 모니터링
Amazon RDS (모든 인스턴스 유형)	CPU 또는 메모리가 한도에 도달함	DB 부하, DB 부하, CPU
RDS for PostgreSQL	높은 복제 슬롯 지연	OldestReplicationSlotLag

DevOps전문가가 모니터링하는 Amazon RDS 인스턴스의 추가 CloudWatch 벤더 메트릭:

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- 실패한 SQL ServerAgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

Performance Insights의 데이터를 사용한 RDS 모니터링

Aurora PostgreSQL, Aurora MySQL 및 PostgreSQL용 RDS와 같은 특정 유형의 Amazon RDS 인스턴스의 경우 해당 인스턴스에 Performance Insights가 활성화되도록 하여 Guru 모니터링에서 더 많은 기능을 활용할 수 있습니다. DevOps

DevOpsGuru는 다음 시나리오를 포함하여 다양한 상황에 대한 사후 대응적 통찰력을 제공합니다.

DevOpsGuru가 반응형 인사이트를 생성하기 위해 식별하는 시나리오
경합 문제 잠금
색인 누락

DevOpsGuru가 반응형 인사이트를 생성하기 위해 식별하는 시나리오
애플리케이션 풀의 잘못된 구성
최적이 아닌 JDBC 기본값

DevOpsGuru는 다음 시나리오를 포함하여 다양한 상황에 대한 사전 예방적 통찰력을 제공합니다.

AWS Guru가 모니터링하는 리소스 DevOps	DevOpsGuru가 사전 예방적 인사이트를 생성하기 위해 파악한 시나리오
Aurora MySQL	InnoDB 히스토리 목록이 너무 커져 데이터베이스 종료 시간이 길어지는 등 성능이 저하될 수 있습니다.
Aurora MySQL	디스크에 생성된 임시 테이블이 증가하여 데이터베이스 성능에 영향을 미칠 수 있음
PostgreSQL용 RDS, Aurora PostgreSQL용 RDS	트랜잭션에서 너무 오랫동안 유휴 상태였던 연결, 잠금 유지, 다른 쿼리 차단, 진공 (autovacuum 포함) 이 데드 행을 정리하지 못하게 할 경우 발생할 수 있는 영향

데이터베이스 작업 모니터링 Amazon Redshift

DevOpsGuru는 CPU 사용률 및 사용된 디스크 공간 비율을 포함한 기본 CloudWatch 메트릭을 수집하여 Amazon Redshift 리소스를 모니터링할 수 있습니다. 이러한 지표는 기본적으로 제공되므로 DevOps Guru가 리소스를 자동으로 모니터링하도록 추가 구성할 필요가 없습니다. Amazon Redshift DevOpsGuru는 과거 패턴을 기반으로 이러한 지표의 기준을 설정하고 이를 실시간 데이터와 비교하여 이상 현상을 감지합니다.

Guru가 식별한 시나리오 DevOps	CloudWatch 지표 모니터링
클러스터 워크로드, 왜곡되고 정렬되지 않은 데이터 또는 리더 노드 작업과 같은 요인으로 인한	CPUUtilization

Guru가 식별한 시나리오 DevOps	CloudWatch 지표 모니터링
Amazon Redshift 인스턴스의 높은 CPU 사용률을 감지합니다.	
쿼리 처리, 배포 및 정렬 키, 유지 관리 작업 또는 툼스톤 블록 관련 문제로 인해 Amazon Redshift 인스턴스의 디스크 공간이 부족한 경우를 감지합니다.	PercentageDiskSpaceUsed

CloudWatch Guru가 모니터링하는 Amazon Redshift 인스턴스의 추가 벤더 메트릭: DevOps

- DatabaseConnections
- HealthStatus
- MaintenanceMode
- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS
- ReadLatency
- WLM QueueLength
- WLM QueueWaitTime
- WLM QueryDuration
- WriteLatency

RDS용 Guru에서 예외 항목 다루기 DevOps

DevOpsGuru는 Amazon RDS 엔진을 포함하여 지원되는 AWS 리소스를 탐지 및 분석하고 이에 대한 권장 사항을 제공합니다. Performance Insights가 활성화된 Amazon Aurora 및 PostgreSQL용 RDS 데이터베이스 인스턴스의 경우 RDS용 Guru는 성능 문제에 대한 상세한 데이터베이스 DevOps 관련 분석을 제공하고 수정 조치를 권장합니다.

주제

- RDS용 Guru 개요 DevOps
- RDS용 Guru DevOps 활성화
- Amazon RDS의 이상 현상 분석

RDS용 Guru 개요 DevOps

아래에서는 RDS용 DevOps Guru의 주요 이점 및 기능에 대한 요약을 확인할 수 있습니다. 인사이트 및 이상 현상에 대한 배경은 DevOps Guru 개념을 참조하십시오.

주제

- RDS를 위한 DevOps Guru의 이점
- 데이터베이스 성능 튜닝의 주요 개념
- RDS용 Guru의 주요 개념 DevOps
- RDS용 DevOps 구루의 작동 방식
- 지원되는 데이터베이스 엔진

RDS를 위한 DevOps Guru의 이점

Amazon RDS 데이터베이스를 담당하는 경우 해당 데이터베이스에 영향을 미치는 이벤트 또는 회귀가 발생하고 있는 것을 알지 못할 수 있습니다. 이 문제에 대해 알아볼 때, 문제가 발생하는 이유나 어떻게 대응해야 할 지 모를 수도 있습니다. 데이터베이스 관리자 (DBA) 에게 도움을 요청하거나 타사 도구를 이용하는 대신 Guru for RDS의 권장 사항을 따를 수 있습니다. DevOps

Guru for RDS의 상세한 분석을 통해 다음과 같은 이점을 얻을 수 DevOps 있습니다.

빠른 진단

DevOpsGuru for RDS는 데이터베이스 원격 분석을 지속적으로 모니터링하고 분석합니다. Performance Insights, 향상된 모니터링 및 Amazon은 데이터베이스 인스턴스에 대한 원격 측정 데이터를 CloudWatch 수집합니다. DevOpsGuru for RDS는 통계 및 기계 학습 기술을 사용하여 이 데이터를 마이닝하고 이상 현상을 탐지합니다. Amazon Aurora 데이터베이스용 원격 분석 데이터에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora에서 성능 개선 도우미 DB 로드 모니터링과 향상된 모니터링을 사용하여 OS 모니터링을 참조하세요. Amazon RDS 데이터베이스용 원격 분석 데이터에 대한 자세한 내용은 Amazon RDS 사용 설명서의 Amazon 관계형 데이터베이스 서비스에서 성능 개선 도우미 DB 로드 모니터링과 향상된 모니터링을 사용한 OS 지표 모니터링을 참조하세요.

빠른 해결

각 이상 현상은 성능 문제를 식별하고 조사 또는 수정 작업 방법을 제안합니다. 예를 들어 DevOps Guru for RDS는 특정 대기 이벤트를 조사하도록 권장할 수 있습니다. 또는 애플리케이션 풀 설정을 조정하여 데이터베이스 연결 수를 제한하도록 권장할 수도 있습니다. 이러한 권장 사항을 기반으로 수동으로 문제를 해결하는 것보다 성능 문제를 더 빨리 해결할 수 있습니다.

사전 예방 인사이트

DevOpsGuru for RDS는 리소스의 메트릭을 사용하여 잠재적으로 문제가 될 수 있는 동작이 더 큰 문제로 확대되기 전에 탐지합니다. 예를 들어, 데이터베이스에 연결된 세션이 활성 작업을 수행하지 않는 경우를 감지하여 데이터베이스 리소스를 차단하고 있을 수 있습니다. DevOps그런 다음 Guru는 문제가 더 커지기 전에 문제를 해결하는 데 도움이 되는 권장 사항을 제공합니다.

Amazon 엔지니어의 깊이 있는 지식과 기계 학습

DevOpsGuru for RDS는 성능 문제를 감지하고 병목 현상을 해결하는 데 도움을 주기 위해 기계 학습 (ML) 및 고급 통계 분석을 사용합니다. Amazon 데이터베이스 엔지니어들은 수년간 수십만 개의 데이터베이스를 관리해 온 결과를 집약한 DevOps Guru for RDS 연구 결과를 개발하는 데 기여했습니다. DevOpsGuru for RDS는 이러한 집단적 지식을 바탕으로 모범 사례를 가르쳐 줄 수 있습니다.

데이터베이스 성능 튜닝의 주요 개념

DevOpsGuru for RDS는 사용자가 몇 가지 주요 성능 개념을 잘 알고 있다고 가정합니다. 이러한 개념에 대해 자세히 알아보려면 Amazon Aurora 사용 설명서의 성능 개선 도우미 개요 또는 Amazon RDS 사용 설명서의 성능 개선 도우미 개요를 참조하십시오.

주제

- 지표
- 문제 감지
- DB 부하
- 대기 이벤트

지표

지표는 시간 순서별 데이터 포인트 집합을 나타냅니다. 지표는 모니터링할 변수로, 데이터 요소는 시간에 따른 변수의 값을 나타내는 것으로 간주합니다. Amazon RDS는 DB 인스턴스가 실행되는 운영 체제(OS) 및 데이터베이스 측정치를 실시간으로 제공합니다. Amazon RDS 콘솔에서 Amazon RDS DB

인스턴스에 대한 모든 시스템 지표 및 프로세스 정보를 볼 수 있습니다. DevOpsGuru for RDS는 이러한 지표 중 일부에 대한 통찰력을 모니터링하고 제공합니다. 자세한 내용은 Amazon Aurora 클러스터의 모니터링 지표 또는 Amazon 관계형 데이터베이스 서비스 인스턴스의 모니터링 지표를 참조하십시오.

문제 감지

DevOpsGuru for RDS는 데이터베이스 및 운영 체제 (OS) 메트릭을 사용하여 문제가 임박했든 진행 중이든 관계없이 중요한 데이터베이스 성능 문제를 탐지합니다. DevOpsGuru for RDS 문제 감지를 위한 두 가지 주요 작동 방식은 다음과 같습니다.

- 임계값 사용
- 이상 사용

임계값으로 문제 감지

임계값은 모니터링된 지표를 평가하는 데 기준이 되는 경계 값입니다. 임계값은 지표 차트에서 정상 동작과 잠재적 문제가 될 수 있는 동작을 구분하는 수평선으로 생각할 수 있습니다. DevOpsGuru for RDS는 특정 메트릭을 모니터링하고 지정된 리소스에서 잠재적으로 문제가 될 것으로 간주되는 수준을 분석하여 임계값을 생성합니다. DevOps그런 다음 Guru for RDS는 새 지표 값이 일정 기간 동안 지속적으로 지정된 임계값을 초과할 경우 DevOps Guru 콘솔에서 통찰력을 생성합니다. 인사이트에는 미래의 데이터베이스 성능에 영향을 미칠 수 있는 요소를 방지하기 위한 권장 사항이 포함되어 있습니다.

예를 들어 DevOps Guru for RDS는 15분 동안 디스크를 사용하는 임시 테이블 수를 모니터링하여 임시 테이블의 초당 디스크 사용률이 비정상적으로 높을 때 통찰력을 얻을 수 있습니다. 디스크의 임시 테이블 사용량이 증가하면 데이터베이스 성능에 영향을 미칠 수 있습니다. DevOpsGuru for RDS는 심각해지기 전에 이 상황을 파악하여 문제를 예방하기 위한 수정 조치를 취할 수 있도록 지원합니다.

이상으로 문제 감지

임계값은 간단하고 효과적으로 데이터베이스 문제를 탐지하는 방법을 제공하지만 일부 상황에서는 이것만으로 충분하지 않습니다. 일일 보고 작업과 같은 알려진 프로세스로 인해 지표 값이 정기적으로 급증하여 잠재적으로 문제가 될 수 있는 동작으로 이어지는 경우가 그 예입니다. 이러한 스파이크가 예상되므로 각 항목에 대한 인사이트와 알림을 생성하는 것은 역효과를 유발하고 알림으로 인한 피로로 이어질 수 있습니다.

그러나 다른 지표보다 훨씬 높거나 더 오래 지속되는 지표는 실제 데이터베이스 성능 문제를 나타낼 수 있기 때문에 이례적인 스파이크를 감지하는 것은 여전히 필요합니다. 이 문제를 해결하기 위해

DevOps Guru for RDS는 특정 메트릭을 모니터링하여 메트릭의 동작이 매우 비정상적이거나 변칙적인 경우 이를 탐지합니다. DevOps그런 다음 Guru는 이러한 이상 현상을 통찰력으로 보고합니다.

예를 들어 DevOps Guru for RDS는 DB 부하가 높을 뿐만 아니라 일반적인 동작에서 크게 벗어날 때 통찰력을 생성할 수 있습니다. 이는 예상치 못한 데이터베이스 작업 속도가 크게 저하되었음을 나타냅니다. DevOpsGuru for RDS를 사용하면 비정상적인 DB 로드 스파이크만 인식하므로 사용자는 정말 중요한 문제에 집중할 수 있습니다.

DB 부하

데이터베이스 튜닝의 핵심 개념은 데이터베이스 부하(DB 로드) 지표입니다. DB 로드는 특정 시점의 데이터베이스 사용량을 나타냅니다. DB 로드가 증가하면 데이터베이스 활동이 증가합니다.

데이터베이스 세션은 관계형 데이터베이스와 애플리케이션의 대화를 나타냅니다. 활성 세션은 데이터베이스 요청을 실행 중인 세션입니다. 세션은 CPU에서 실행 중이거나 리소스가 계속 진행될 수 있도록 대기 중일 때 활성화됩니다. 예를 들어 활성 세션은 페이지가 메모리로 읽힐 때까지 기다린 다음 페이지에서 데이터를 읽는 동안 CPU를 사용할 수 있습니다.

성능 개선 도우미의 `DBLoad` 지표는 평균 활성 세션(AAS)으로 측정됩니다. AAS를 계산하기 위해 성능 개선 도우미는 활성 세션 수를 매초마다 샘플링합니다. AAS는 특정 기간 동안의 총 세션 수를 총 샘플 수로 나눈 값입니다. AAS 값이 2이면 평균적으로 2회의 세션이 요청 활성화 상태였음을 의미합니다.

DB 로드는 창고의 활동에 비유할 수 있습니다. 창고에 100명의 근로자를 고용한다고 가정합니다. 한 주문이 들어오면 한 명의 작업자가 주문을 이행하고 다른 작업자는 유휴 상태입니다. 100개 또는 그 이상 주문이 접수되면 100명의 작업자 모두가 동시에 주문을 처리합니다. 지정된 기간 동안 활성 상태의 작업자 수를 주기적으로 샘플링하는 경우 평균 활성 근로자 수를 계산할 수 있습니다. 계산에 따르면 평균적으로 N명의 근로자가 주어진 시간에 주문을 이행하는 중입니다. 어제 평균 근로자가 50명이고 오늘 75명의 근로자라면 창고의 활동 수준은 높아진 것입니다. 마찬가지로 세션 활동이 증가함에 따라 DB 로드가 증가합니다.

자세한 내용은 Amazon Aurora 사용 설명서의 데이터베이스 로드 또는 Amazon RDS 사용 설명서의 데이터베이스 로드를 참조하십시오.

대기 이벤트

대기 이벤트는 데이터베이스 세션이 진행할 수 있도록 대기 중인 리소스를 알려주는 일종의 데이터베이스 계측입니다. 성능 개선 도우미는 활성 세션을 계산하여 데이터베이스 부하를 계산할 때 활성 세션을 기다리게 하는 대기 이벤트도 기록합니다. 이 기법을 사용하면 성능 개선 도우미에서 DB 로드에 영향을 미치는 대기 이벤트를 확인할 수 있습니다.

모든 활성 세션이 CPU에서 실행 중이거나 대기 중입니다. 예를 들어 세션은 메모리를 검색하거나 계산을 수행하거나 프로시저 코드를 실행할 때 CPU를 사용합니다. 세션에서 CPU를 사용하지 않는 경우, 읽을 데이터 파일 또는 기록할 로그가 나올 때까지 대기할 수 있습니다. 세션이 리소스를 기다리는 시간이 길수록 CPU에서 실행되는 시간이 줄어듭니다.

데이터베이스를 튜닝할 때 세션이 기다리는 리소스를 찾으려고 하는 경우가 많습니다. 예를 들어 두 개 또는 세 개의 대기 이벤트가 DB 로드의 90%를 차지할 수 있습니다. 이 측정은 평균적으로 활성 세션이 소수의 리소스를 기다리는 데 대부분의 시간을 소비한다는 것을 의미합니다. 이러한 대기의 원인을 찾을 수 있는 경우, 문제를 해결할 수 있습니다.

창고 작업자 비유를 기억하세요. 책에 대한 주문이 들어옵니다. 작업자의 주문 이행은 지연될 수 있습니다. 예를 들어 다른 작업자가 현재 선반을 재입고 중이거나 트롤리를 사용하지 못할 수 있습니다. 또는 주문 상태를 입력하는 데 사용된 시스템이 느릴 수 있습니다. 작업자가 기다리는 시간이 길수록 주문을 이행하는 것이 더 오래 걸립니다. 대기는 창고 워크플로의 자연스러운 부분이지만 대기 시간이 지나치게 되면 생산성이 떨어집니다. 같은 방식으로 세션 대기가 반복되거나 길면 데이터베이스 성능이 저하될 수 있습니다.

Amazon Aurora의 대기 이벤트에 관한 자세한 내용은 Amazon Aurora 사용 설명서의 Aurora PostgreSQL의 대기 이벤트를 사용한 튜닝과 Aurora MySQL의 대기 이벤트를 사용한 튜닝을 참조하세요.

다른 Amazon RDS 데이터베이스의 대기 이벤트에 대한 자세한 내용은 Amazon RDS 사용 설명서의 RDS for PostgreSQL의 대기 이벤트를 사용한 튜닝을 참조하십시오.

RDS용 Guru의 주요 개념 DevOps

DevOpsGuru는 운영 애플리케이션에서 비정상적이거나 문제가 있는 동작을 감지하면 인사이트를 생성합니다. 인사이트는 하나 이상의 리소스에 대한 이상 징후를 포함합니다. 예외 항목은 Guru가 탐지한 예상치 못하거나 특이한 하나 이상의 관련 지표를 나타냅니다. DevOps

인사이트의 심각도는 높음, 보통 또는 낮음입니다. 인사이트 심각도는 인사이트 생성에 기여한 가장 심각한 이상 현상에 따라 결정됩니다. 예를 들어, 인사이트 AWS-ECS_ MemoryUtilization _and_others에 심각도가 낮은 예외 항목 하나와 심각도가 높은 예외 항목 하나가 포함되어 있는 경우 인사이트의 전체 심각도는 높습니다.

Amazon RDS DB 인스턴스에 Performance Insights가 켜져 있는 경우 RDS용 DevOps Guru는 이러한 인스턴스의 이상 현상에 대한 자세한 분석 및 권장 사항을 제공합니다. 예외 항목을 식별하기 위해 DevOps Guru for RDS는 데이터베이스 지표 값에 대한 기준을 개발합니다. DevOps그런 다음 Guru for RDS는 현재 지표 값을 과거 기준과 비교합니다.

주제

- 사전 예방 인사이트
- 사후 대응 인사이트
- 추천

사전 예방 인사이트

사전 예방 인사이트를 통해 문제가 발생하기 전에 문제를 일으킬 수 있는 행동을 파악할 수 있습니다. 여기에는 더 큰 문제가 발생하기 전에 이를 해결하는 데 도움이 되는 권장 사항 및 관련 지표가 포함된 이상 항목이 포함되어 있습니다.

각 사전 예방 인사이트 페이지에는 한 가지 이상 항목에 대한 세부 정보가 제공됩니다.

사후 대응 인사이트

사후 대응 인사이트는 비정상적인 동작이 발생하는 즉시 이를 식별합니다. 여기에는 현재 문제를 이해하고 해결하는 데 도움이 되는 권장 사항, 관련 지표, 이벤트와 같은 이상 항목이 포함되어 있습니다.

일반적인 이상

캐주얼 이상 항목은 사후 대응 인사이트 내에서 최상위 이상 항목입니다. 이는 Guru 콘솔의 예외 항목 세부 정보 페이지에 기본 지표로 표시됩니다. DevOps 데이터베이스 로드 (DB 로드) 는 RDS용 Guru의 원인적 변칙입니다. DevOps 예를 들어, Insight AWS-ECS_ MemoryUtilization _and_others에는 몇 가지 지표 이상이 있을 수 있는데, 그 중 하나는 리소스 AWS/RDS에 대한 데이터베이스 로드 (DB 로드) 입니다.

인사이트 내에서 여러 Amazon RDS DB 인스턴스에 대한 비정상적인 데이터베이스 로드(DB 로드)가 발생할 수 있습니다. 이상 현상의 심각도는 각 DB 인스턴스마다 다를 수 있습니다. 예를 들어 한 DB 인스턴스의 심각도는 높지만 다른 DB 인스턴스의 심각도는 낮을 수 있습니다. 콘솔은 심각도가 가장 높은 이상 항목을 기본값으로 설정합니다.

문맥적 이상

컨텍스트 이상 항목은 데이터베이스 로드(DB 로드) 내의 결과로, 사후 대응 인사이트와 관련이 있습니다. Guru 콘솔의 예외 항목 세부 정보 페이지에 있는 관련 지표 섹션에 표시됩니다. DevOps 각 문맥적 이상은 조사가 필요한 특정 Amazon RDS 성능 문제를 설명합니다. 예를 들어 인과 관계 이상에는 다음과 같은 문맥적 이상이 포함될 수 있습니다.

- CPU 용량 초과 - CPU 실행 대기열 또는 CPU 사용률이 정상보다 높습니다.
- 데이터베이스 메모리 부족 - 프로세스에 메모리가 충분하지 않습니다.
- 데이터베이스 연결 스파이크 — 데이터베이스 연결 수가 정상보다 많습니다.

추천

각 인사이트에는 하나 이상의 권장 조치가 있습니다. 다음 예는 DevOps Guru에서 RDS용으로 생성한 권장 사항입니다.

- SQL ID *List_of_IDs*를 조정하여 CPU 사용량을 줄이거나 인스턴스 유형을 업그레이드하여 CPU 용량을 늘리십시오.
- 현재 데이터베이스 연결과 관련된 스파이크를 검토하세요. 새 데이터베이스 연결이 자주 동적으로 할당되지 않도록 응용 프로그램 풀 설정을 조정하는 것을 고려하십시오.
- 메모리 내 정렬이나 대규모 조인과 같이 과도한 메모리 작업을 수행하는 SQL 명령문을 찾아보세요.
- *List_of_IDs*와 같은 SQL ID의 I/O 사용량이 많은지 조사해 보세요.
- 대규모 정렬을 수행하거나 큰 임시 테이블을 사용하는 명령문과 같이 대량의 임시 데이터를 생성하는 명령문이 있는지 확인하세요.
- 애플리케이션을 검사하여 데이터베이스 워크로드 증가의 원인을 확인하십시오.
- MySQL 성능 스키마 활성화를 고려하십시오.
- 오래 실행되는 트랜잭션이 있는지 확인하고 커밋 또는 롤백으로 이를 종료하십시오.
- 지정된 시간보다 오래 '트랜잭션 유휴' 상태로 유지된 모든 세션을 종료하려면 idle_in_transaction_session_timeout 매개 변수를 구성하세요.

RDS용 DevOps 구루의 작동 방식

DevOpsGuru for RDS는 지표 데이터를 수집하여 분석한 다음 대시보드에 예외 항목을 게시합니다.

주제

- 데이터 수집 및 분석
- 이상 게시

데이터 수집 및 분석

DevOpsRDS용 Guru는 Amazon RDS Performance Insights에서 Amazon RDS 데이터베이스에 대한 데이터를 수집합니다. 이 기능을 사용하면 Amazon RDS DB 인스턴스를 모니터링하고, 지표를 수집하고, 차트로 지표를 탐색할 수 있습니다. 가장 중요한 성능 지표는 다음과 같습니다. DBLoad DevOpsGuru for RDS는 Performance Insights 지표를 사용하고 이를 분석하여 이상 징후를 탐지합니다. 성능 개선 도우미에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora에서 성능 개선 도우미를 사용해 DB 로드 모니터링 또는 Amazon RDS 사용 설명서의 Amazon프ㄴ RDS에서 성능 개선 도우미를 사용해 DB 로드 모니터링을 참조하십시오.

DevOpsGuru for RDS는 기계 학습과 고급 통계 분석을 사용하여 Performance Insights에서 수집한 데이터를 분석합니다. DevOpsGuru for RDS는 성능 문제를 발견하면 다음 단계로 진행합니다.

이상 게시

높은 DB 로드와 같은 데이터베이스 성능 문제로 인해 데이터베이스의 서비스 품질이 저하될 수 있습니다. DevOpsGuru는 RDS 데이터베이스에서 문제를 감지하면 대시보드에 인사이트를 게시합니다. 인사이트에는 리소스 AWS/RDS에 대한 이상 항목이 포함되어 있습니다.

인스턴스에 대해 성능 개선 도우미가 켜져 있는 경우 이상 현상에 문제에 대한 자세한 분석이 포함됩니다. DevOps또한 Guru for RDS는 조사 또는 특정 수정 조치를 수행할 것을 권장합니다. 예를 들어, 부하가 높은 특정 SQL 문을 조사하거나, CPU 용량을 늘리거나, 세션을 종료하는 것이 권장될 수 있습니다. idle-in-transaction

지원되는 데이터베이스 엔진

DevOpsGuru for RDS는 다음 데이터베이스 엔진에서 지원됩니다.

MySQL과 호환되는 Amazon Aurora

이 엔진에 대해 자세히 알아보려면 Amazon Aurora 사용 설명서의 Amazon Aurora MySQL 사용을 참조하십시오.

Amazon Aurora의 PostgreSQL 호환성

이 엔진에 대해 자세히 알아보려면 Amazon Aurora 사용 설명서의 Amazon Aurora PostgreSQL 사용을 참조하십시오.

Amazon RDS for PostgreSQL 호환성 지원

이 엔진에 대한 자세한 내용은 Amazon RDS 사용 설명서에서 Amazon RDS for PostgreSQL을 참조하십시오.

DevOpsGuru는 이상 현상을 보고하고 다른 데이터베이스 엔진에 대한 기본 분석을 제공합니다. DevOpsRDS용 Guru는 Amazon Aurora 및 PostgreSQL 인스턴스용 RDS에 대해서만 자세한 분석 및 권장 사항을 제공합니다.

RDS용 Guru DevOps 활성화

RDS용 DevOps Guru를 활성화하면 DevOps Guru가 DB 인스턴스와 같은 리소스의 이상 현상을 분석할 수 있습니다. Amazon RDS를 사용하면 RDS DB 인스턴스 또는 DB 클러스터의 권장 기능을 쉽게 검색하고 활성화할 수 있습니다. 이를 위해 RDS는 Amazon EC2 DevOps, Guru, IAM과 같은 다른 서

비스에 API를 호출합니다. RDS 콘솔이 이러한 API 호출을 수행하면, AWS CloudTrail이 이를 기록하여 가시성을 확보합니다.

DevOpsGuru가 Amazon RDS 데이터베이스에 대한 통찰력을 게시하도록 허용하려면 다음 섹션의 작업을 완료하십시오.

주제

- Amazon RDS DB 인스턴스에 대한 성능 개선 도우미 활성화
- RDS용 DevOps Guru에 대한 액세스 정책 구성
- Amazon RDS DB 인스턴스를 DevOps Guru 커버리지에 추가

Amazon RDS DB 인스턴스에 대한 성능 개선 도우미 활성화

RDS용 DevOps Guru가 DB 인스턴스의 이상 현상을 분석하도록 하려면 Performance Insights가 켜져 있어야 합니다. DB 인스턴스에 대해 Performance Insights가 켜져 있지 않은 경우 RDS용 DevOps Guru는 다음 위치에서 사용자에게 알립니다.

대시보드

리소스 유형별로 인사이트를 보는 경우 RDS 타일에 성능 개선 도우미가 켜져 있지 않다는 알림이 표시됩니다. 링크를 선택하여 Amazon RDS 콘솔에서 성능 개선 도우미를 활성화하십시오.

인사이트

페이지 하단의 권장 사항 섹션에서 Amazon RDS 성능 개선 도우미 활성화를 선택합니다.

설정

서비스: Amazon RDS 섹션에서 링크를 선택하여 Amazon RDS 콘솔의 성능 개선 도우미를 활성화합니다.

자세한 내용은 Amazon Aurora 사용 설명서의 성능 개선 도우미 활성화 및 비활성화 또는 Amazon RDS 사용 설명서의 성능 개선 도우미 활성화를 참조하십시오.

RDS용 DevOps Guru에 대한 액세스 정책 구성

사용자가 RDS용 DevOps Guru에 액세스하려면 다음 정책 중 하나의 권한이 있어야 합니다.

- AWS 관리형 정책 `AmazonRDSFullAccess`
- 다음 작업을 허용하는 고객 관리형 정책입니다.

- `pi:GetResourceMetrics`
- `pi:DescribeDimensionKeys`
- `pi:GetDimensionKeyDetails`

자세한 내용은 Amazon Aurora 사용 설명서의 성능 개선 도우미 액세스 정책 구성 또는 Amazon RDS 사용 설명서의 성능 개선 도우미 액세스 정책 구성을 참조하십시오.

Amazon RDS DB 인스턴스를 DevOps Guru 커버리지에 추가

DevOpsGuru 콘솔 또는 Amazon RDS 콘솔에서 Amazon RDS 데이터베이스를 모니터링하도록 DevOps Guru를 구성할 수 있습니다.

DevOpsGuru 콘솔에는 다음과 같은 옵션이 있습니다.

- 계정 수준에서 DevOps Guru를 켜세요. 이 값이 기본값입니다. 이 옵션을 선택하면 DevOps Guru는 Amazon RDS 데이터베이스를 포함하여 AND에서 지원되는 모든 AWS 리소스를 분석합니다. AWS 리전 AWS 계정
- RDS용 DevOps Guru의 AWS CloudFormation 스택을 지정하십시오.

  자세한 설명은 AWS CloudFormation 스택을 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다. 섹션을 참조하세요.
- Amazon RDS 리소스를 태그합니다.

  태그는 사용자 또는 AWS 리소스에 할당하는 사용자 지정 속성 레이블입니다. 태그를 사용하여 애플리케이션을 구성하는 AWS 리소스를 식별합니다. 그런 다음 태그별로 인사이트를 필터링하여 애플리케이션에서 생성된 인사이트만 볼 수 있습니다. 애플리케이션의 Amazon RDS 리소스에서 생성된 인사이트만 보려면 Amazon RDS 리소스 `Devops-guru-rds` 태그와 같은 값을 추가하십시오. 자세한 설명은 태그를 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다. 섹션을 참조하세요.

> **Note**
>
> Amazon RDS 리소스에 태그를 지정할 때는 클러스터가 아닌 데이터베이스 인스턴스에 태그를 지정해야 합니다.

Amazon RDS 콘솔에서 DevOps Guru 모니터링을 활성화하려면 RDS 콘솔에서 DevOps Guru 켜기를 참조하십시오. Amazon RDS 콘솔에서 DevOps Guru를 활성화하려면 태그를 사용해야 한다는 점에 유

의하십시오. 태그에 대한 자세한 내용은 the section called “태그를 사용하여 애플리케이션의 리소스를 식별합니다.” 단원을 참조하십시오.

Amazon RDS의 이상 현상 분석

DevOpsGuru for RDS가 대시보드에 성능 이상을 게시할 때는 일반적으로 다음 단계를 수행합니다.

1. Guru 대시보드에서 인사이트를 확인하세요. DevOps DevOpsGuru for RDS는 사후 대응적 인사이트와 사전 예방적 통찰력을 모두 보고합니다.

   자세한 설명은 인사이트 보기 섹션을 참조하세요.
2. AWS/RDS 리소스의 이상 항목을 확인하십시오.

   자세한 내용은 사후 대응 인사이트 보기 및 사전 예방 이상 항목 보기 섹션을 참조하세요.
3. DevOpsGuru의 RDS 권장 사항에 응답하세요.

   자세한 설명은 권장 사항 대응 섹션을 참조하세요.
4. DB 인스턴스의 상태를 모니터링하여 해결된 성능 문제가 재발하지 않도록 하십시오.

   자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora DB 클러스터의 모니터링 지표 및 Amazon RDS 사용 설명서의 Amazon RDS 인스턴스 모니터링 지표를 참조하십시오.

인사이트 보기

DevOpsGuru 콘솔의 Insights 페이지에 액세스하여 사후 대응적이고 능동적인 통찰력을 찾아보세요. 이 목록에서 인사이트를 선택하여 지표, 권장 사항 및 인사이트에 대한 추가 정보가 포함된 세부 정보 페이지를 볼 수 있습니다.

인사이트를 보려면

1. https://console.aws.amazon.com/devops-guru/ 에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 사후 대응 탭을 선택하여 사후 대응 인사이트를 확인하거나, 사전 예방을 선택하여 사전 예방 인사이트를 확인하십시오.
4. 상태 및 심각도별로 우선순위를 정하여 인사이트 이름을 선택합니다.

   자세한 인사이트 페이지가 나타납니다.

사후 대응 인사이트 보기

인사이트 내에서 Amazon RDS 리소스의 이상 현상을 확인할 수 있습니다. 사후 대응 인사이트 페이지의 집계된 지표 섹션에서 해당 타임라인과 함께 이상 항목 목록을 볼 수 있습니다. 이상 항목과 관련된 로그 그룹 및 이벤트에 대한 정보를 표시하는 섹션도 있습니다. 사후 대응 인사이트의 인과 변칙 각각에는 이상 항목에 대한 세부 정보가 포함된 해당 페이지가 있습니다.

RDS 사후 대응 이상 항목에 대한 세부 분석 보기

이 단계에서는 이상 항목을 자세히 분석하여 Amazon RDS DB 인스턴스에 대한 자세한 분석 및 권장 사항을 확인하십시오.

세부 분석은 성능 개선 도우미가 활성화된 Amazon RDS DB 인스턴스에서만 사용할 수 있습니다.

이상 항목 세부 정보 페이지를 자세히 살펴보려면

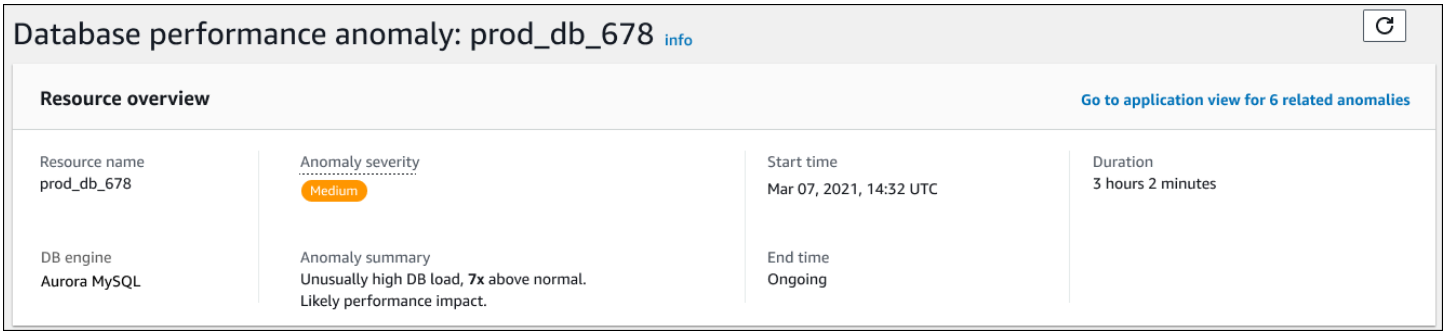
1. 인사이트 페이지에서 리소스 유형이 AWS/RDS로 집계된 지표 찾으세요.
2. 세부 정보 보기를 선택합니다.

   이상 항목의 세부 정보 페이지가 나타납니다. 제목은 데이터베이스 성능 이상 현상으로 시작하며 리소스 이름이 나타납니다. 콘솔은 이상 항목 발생 시기에 관계없이 심각도가 가장 높은 이상 항목을 기본값으로 설정합니다.
3. (선택 사항) 여러 리소스가 영향을 받는 경우 페이지 상단의 목록에서 다른 리소스를 선택합니다.

다음에서 세부 정보 페이지의 구성 요소에 대한 설명을 확인할 수 있습니다.

리소스 개요

세부정보 페이지의 상단 섹션은 리소스 개요입니다. 이 섹션에서는 Amazon RDS DB 인스턴스에서 발생하는 성능 이상에 대해 요약합니다.

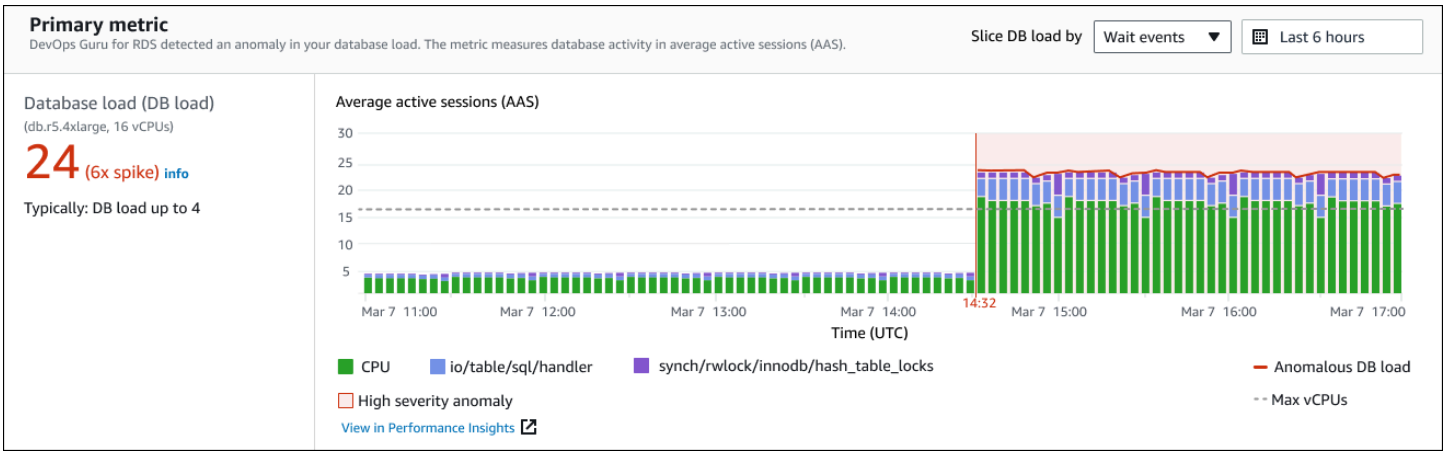


이 섹션은 다음 필드를 포함합니다.

- 리소스 이름 - 이상 현상이 발생한 DB 인스턴스의 이름입니다. 이 예시에서 리소스의 이름은 prod_db_678입니다.
- DB 엔진 — 이상 현상이 발생한 DB 인스턴스의 이름입니다. 이 예시에서 엔진은 Aurora MySQL입니다.
- 이상 심각도 — 이상 징후가 인스턴스에 미치는 부정적인 영향을 측정한 것입니다. 가능한 심각도는 높음, 보통 및 낮음입니다.
- 이상 항목 요약 — 문제에 대한 간략한 요약입니다. 일반적인 요약은 비정상적으로 높은 DB 로드입니다.
- 시작 시간 및 종료 시간 — 이상 현상이 시작되고 종료된 시간입니다. 종료 시간이 진행 중이면, 이상 현상이 계속 발생하고 있는 것입니다.
- 지속 시간 — 이상 동작의 지속 시간입니다. 이 예시에서는 이상 현상이 진행 중이며 3시간 2분 동안 발생했습니다.

기본 지표

기본 지표 섹션에는 인사이트 내의 최상위 이상 항목인 인과적 이상 항목이 요약되어 있습니다. 인과적 이상은 DB 인스턴스에서 발생하는 일반적인 문제라고 생각하면 됩니다.



왼쪽 패널은 이 문제에 대한 자세한 내용을 제공합니다. 이 예시의 요약에는 다음 정보가 포함됩니다.

- 데이터베이스 로드(DB 로드) - 이상 현상을 데이터베이스 로드 문제로 분류한 것입니다. 성능 개선 도우미의 해당 지표는 DBLoad입니다. 이 지표는 Amazon에도 CloudWatch 게시됩니다.
- db.r5.4xlarge - DB 인스턴스 클래스입니다. vCPU 수(이 예시에서는 16개)는 평균 활성 세션(AAS) 차트의 점선에 해당합니다.

- 24(6x 스파이크) — 인사이트에 보고된 시간 간격 동안 평균 활성 세션(AAS)으로 측정한 DB 부하입니다. 따라서 이상 현상이 발생한 기간 중 특정 시점에 데이터베이스에서 평균 24개의 세션이 활성 상태였습니다. 이 인스턴스의 DB 로드는 일반 DB 로드의 6배입니다.
- 일반적으로 DB 로드 최대 4개 — 일반적인 워크로드 중 DB 부하의 기준선(AAS로 측정됨)입니다. 값 4는 정상 운영 중에 데이터베이스에서 특정 시점에 활성 상태인 세션이 평균 4개 이하임을 의미합니다.

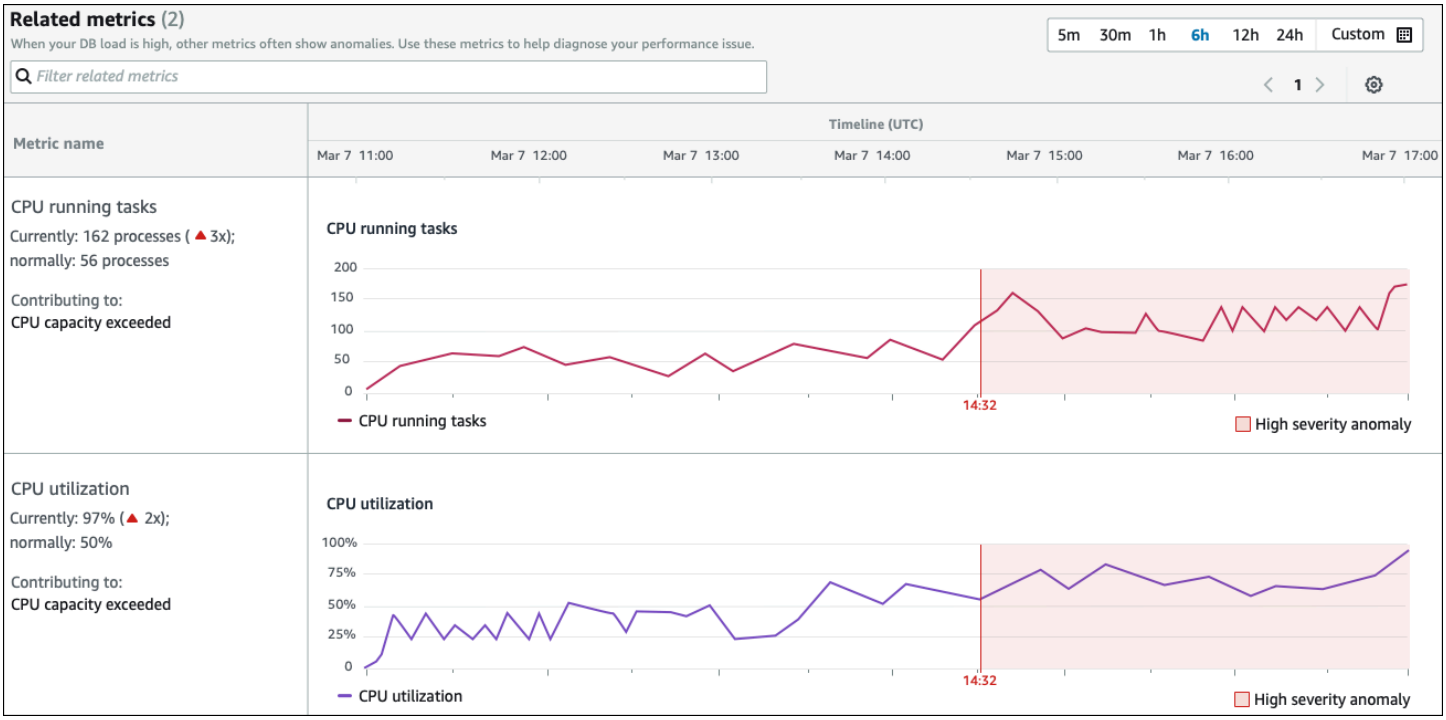
로드 차트는 기본적으로 대기 이벤트를 기준으로 분할됩니다. 즉, 차트의 각 막대에서 가장 큰 색상 영역은 전체 DB 로드에 가장 많이 기여하는 대기 이벤트를 나타냅니다. 차트에는 문제가 시작된 시간(빨간색)이 표시됩니다. 막대에서 가장 많은 공간을 차지하는 대기 이벤트에 주의를 기울이세요.

- `CPU`
- `IO:wait/io/sql/table/handler`

이 Aurora MySQL 데이터베이스에서 이전 대기 이벤트가 정상보다 많이 나타납니다. Amazon Aurora의 대기 이벤트를 사용해 성능을 조정하는 자세한 방법은 Amazon Aurora 사용 설명서의 Aurora MySQL 대기 이벤트를 사용한 튜닝과 Aurora PostgreSQL 대기 이벤트를 사용한 튜닝을 참조하세요. RDS for PostgreSQL에서 대기 이벤트를 사용하여 성능을 조정하는 방법을 알아보려면 Amazon RDS 사용 설명서의 RDS for PostgreSQL의 대기 이벤트를 사용한 튜닝을 참조하십시오.

관련 지표

관련 지표 섹션에는 인과적 이상 항목 내에서 구체적으로 발견된 문맥적 이상이 나열되어 있습니다. 이러한 결과는 성능 문제에 대한 추가 정보를 제공합니다.



관련 지표 테이블에는 다음 두 개의 열이 있습니다: 지표 이름 및 타임라인 (UTC). 테이블의 모든 행은 특정 지표에 해당합니다.

모든 행의 첫 번째 열에는 다음과 같은 정보가 있습니다.

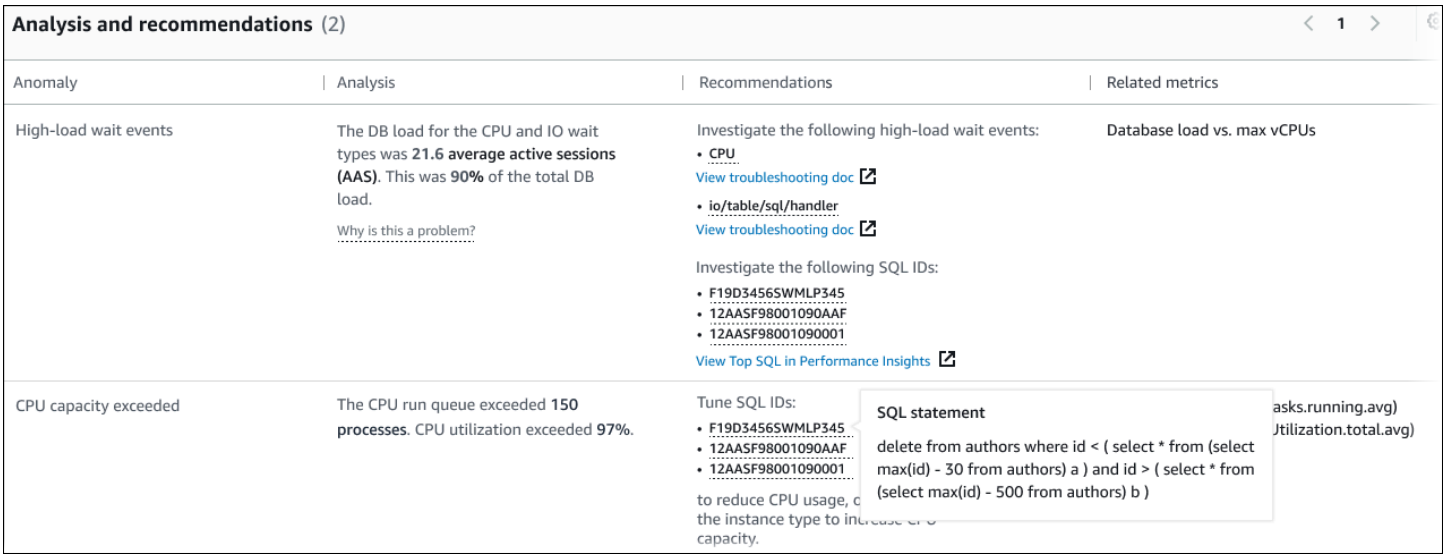
- ## – 지표의 이름입니다. 첫 번째 행은 지표를 CPU 실행 작업으로 식별합니다.
- 현재 — 지표의 현재 값입니다. 첫 번째 행의 현재 값은 162개 프로세스(3x) 입니다.
- 일반적으로 — 이 데이터베이스가 정상적으로 작동할 때의 이 지표의 기준입니다. DevOpsGuru for RDS는 1주간의 기록 기간 동안의 95번째 백분위수 값으로 기준선을 계산합니다. 첫 번째 행은 CPU에서 일반적으로 56개의 프로세스가 실행되고 있음을 나타냅니다.
- 기여 - 이 지표와 관련된 조사 결과입니다. 첫 번째 행에서 CPU 실행 중인 작업 지표는 CPU 용량 초과 이상과 연관되어 있습니다.

타임라인 열에는 지표의 선형 차트가 표시됩니다. 음영 영역은 DevOps Guru for RDS에서 해당 결과를 심각도 높음으로 지정한 시간 간격을 나타냅니다.

분석 및 권장 사항

인과적 이상은 전체 문제를 설명하는 반면, 문맥적 이상은 조사가 필요한 특정 결과를 설명합니다. 각 조사 결과는 일련의 관련 지표에 해당합니다.

분석 및 권장 사항 섹션의 다음 예시에서는 DB 로드가 높은 이상 현상에 대한 두 가지 결과가 있습니다.



이 표에는 다음과 같은 열이 있습니다.

- 이상 항목 — 이 문맥적 이상 현상에 대한 일반적인 설명입니다. 이 예시에서 첫 번째 이상은 로드가 높은 대기 이벤트이고, 두 번째 이상은 CPU 용량 초과입니다.
- 분석 — 이상 현상에 대한 자세한 설명입니다.

  첫 번째 이상 사례에서는 세 가지 대기 유형이 DB 로드의 90%를 차지합니다. 두 번째 이상 사례에서는 CPU 실행 대기열이 150을 초과했습니다. 즉, 주어진 시간에 150개 이상의 세션이 CPU 시간을 기다리고 있다는 말입니다. CPU 사용률이 97%를 넘었다는 것은, 문제가 발생한 기간 동안 CPU가 사용 중인 시간의 97%를 초과했음을 의미합니다. 따라서 평균 150개의 세션이 CPU에서 실행되기를 기다리는 동안 CPU는 거의 계속 점유되고 있었습니다.
- 권장 사항 — 이상 현상에 대한 권장 사용자 대응입니다.

  첫 번째 예외 현상에서 DevOps Guru for RDS는 대기 이벤트 및 을 조사할 것을 권장합니다. `cpu` `io/table/sql/handler` 이러한 이벤트를 기반으로 데이터베이스 성능을 조정하는 방법을 알아보려면 Amazon Aurora 사용 설명서의 cpu 및 io/table/sql/handler를 참조하십시오.

  두 번째 예외 현상에서 DevOps Guru for RDS는 세 개의 SQL 문을 튜닝하여 CPU 사용량을 줄일 것을 권장합니다. 링크 위로 마우스를 가져가면 SQL 텍스트를 볼 수 있습니다.
- 관련 지표 - 이상 현상에 대한 구체적인 측정치를 제공하는 지표입니다. 이러한 지표에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora 지표 참조 또는 Amazon RDS 사용 설명서의 Amazon RDS 지표 참조를 확인하십시오.

첫 번째 예외 현상에서 DevOps Guru for RDS는 DB 부하를 인스턴스의 최대 CPU와 비교할 것을 권장합니다. 두 번째 이상 상황의 경우 CPU 실행 대기열, CPU 사용률, SQL 실행 속도를 살펴보는 것이 좋습니다.

사전 예방 이상 항목 보기

인사이트 내에서 Amazon RDS 리소스의 이상 항목을 확인할 수 있습니다. 각 사전 예방 인사이트는 사전 예방 이상 항목 하나에 대한 세부 정보를 제공합니다. 사전 예방 인사이트 페이지에서는 인사이트 개요, 이상 현상에 대한 세부 지표, 향후 문제 방지를 위한 권장 사항을 확인할 수 있습니다. 사전 예방 이상 항목을 보려면 사전 예방 인사이트 페이지로 이동하십시오.

인사이트 개요

인사이트 개요 섹션에서는 인사이트가 생성된 이유에 대한 세부 정보를 제공합니다. 여기에는 인사이트의 심각도뿐만 아니라 이상 항목에 대한 설명, 이상 항목이 발생한 시기의 시간대도 표시됩니다. 또한 Guru에서 탐지한 영향을 받는 서비스 및 애플리케이션 수를 나열합니다. DevOps

지표

지표 섹션은 이상 현상에 대한 그래프를 제공합니다. 각 그래프에는 리소스의 기준 동작에 따라 결정된 임계값과 이상 발생 시점부터 보고된 지표 데이터가 표시됩니다.

집계된 리소스에 대한 권장 사항

이 섹션에서는 보고된 문제가 더 큰 문제로 확대되기 전에 이를 완화하기 위해 취할 수 있는 조치를 제안합니다. 가능한 조치는 권장 사용자 지정 변경 열에 나와 있습니다. 권장 사항의 근거는 DevOps Guru가 이를 권장하는 이유에 나와 있습니다. 칼럼. 권장 사항에 대응하는 방법에 대한 자세한 내용은 the section called “권장 사항 대응”을 참조하세요.

권장 사항 대응

권장 사항은 인사이트에서 가장 중요한 부분입니다. 이 분석 단계에서는 성능 문제를 해결하기 위해 조치를 취합니다. 일반적으로 다음 단계를 수행합니다.

1. 보고된 성능 문제가 실제 문제를 나타내는지 여부를 결정하십시오.

   경우에 따라 문제가 예상되지만 심각할 수도 있습니다. 예를 들어 테스트 데이터베이스에 극심한 DB 부하가 발생하는 경우 DevOps Guru for RDS는 해당 부하를 성능 이상으로 보고합니다. 하지만 이 이상 현상은 예상된 테스트 결과이므로 수정할 필요가 없습니다.

   문제에 대한 대응이 필요하다고 판단되면 다음 단계로 이동합니다.

2. 권장 사항을 구현할지 여부를 결정하십시오.

   권장 사항 테이블의 열에는 권장 조치가 표시됩니다. 사후 대응 인사이트의 경우 사후 대응 이상 세부 정보 페이지의 권장 사항 열을 확인하세요. 사전 예방 인사이트의 경우 사전 예방 인사이트 페이지의 권장 사용자 지정 변경 열을 확인하세요.

   DevOpsGuru for RDS는 몇 가지 잠재적인 문제 시나리오를 다루는 권장 사항 목록을 제공합니다. 이 목록을 검토한 후 현재 상황에 더 적합한 권장 사항을 결정하고 적용을 고려하세요. 권장 사항이 상황에 적합한 경우 다음 단계를 진행합니다. 그렇지 않은 경우 나머지 단계를 건너뛰고 수동으로 문제를 해결하세요.

3. 권장 조치를 수행하십시오.

   DevOpsGuru for RDS는 다음 중 하나를 수행할 것을 권장합니다.

   - 구체적인 수정 조치를 수행하십시오.

     예를 들어 DevOps Guru for RDS는 CPU 용량을 업그레이드하거나, 애플리케이션 풀 설정을 조정하거나, 성능 스키마를 사용하도록 권장할 수 있습니다.

   - 문제의 원인을 조사하십시오.

     일반적으로 DevOps Guru for RDS는 특정 SQL 문이나 대기 이벤트를 조사할 것을 권장합니다. 예를 들어 대기 이벤트 `io/table/sql/handler` 조사가 권장될 수 있습니다. Amazon Aurora 사용 설명서의 Aurora PostgreSQL 대기 이벤트 튜닝 또는 Aurora MySQL 대기 이벤트 튜닝, 또는 Amazon RDS 사용 설명서의 RDS for PostgreSQL 대기 이벤트 튜닝에서 나열된 대기 이벤트를 찾아보세요. 그런 다음 권장 조치를 수행하십시오.

     > **Important**
     >
     > 프로덕션 인스턴스를 변경하기 전에 테스트 인스턴스에서 변경 사항을 테스트하는 것이 좋습니다. 이러한 방식으로 변경의 영향을 이해하게 됩니다.

Guru를 사용한 비관계형 데이터베이스 모니터링 DevOps

DevOpsGuru는 모범 사례에 따라 리소스를 구성하는 데 도움이 되는 비관계형 또는 NoSQL 데이터베이스에 대한 통찰력을 생성할 수 있습니다. 예를 들어 DevOps Guru는 기존 트래픽을 기반으로 미래의 요구 사항을 예측하여 용량 계획을 완벽하게 수립하는 데 도움을 줄 수 있습니다. DevOpsGuru는 구성한 것보다 적은 리소스를 사용하고 있는지 파악하고 과거 사용량을 기반으로 애플리케이션 가용성을 개선하기 위한 권장 사항을 제공할 수 있습니다. 이를 통해 불필요한 비용을 줄일 수 있습니다.

DevOpsGuru는 용량 계획 외에도 스로틀링, 트랜잭션 충돌, 조건부 검사 실패, SDK 파라미터의 개선이 필요한 영역 등과 같은 운영 문제를 탐지하고 문제를 해결할 수 있도록 지원합니다. 데이터베이스는 일반적으로 여러 서비스 및 리소스와 연결되며 DevOps Guru는 태그 지정 또는 집계에 기반한 그룹을 사용하여 애플리케이션 구조의 상관 관계를 분석할 수 있습니다. AWS CloudFormation 이상 현상에는 동일한 솔루션의 영향을 받는 여러 리소스가 포함될 수 있습니다. DevOpsGuru는 다양한 리소스 메트릭, 구성, 로그 및 이벤트 간에 상관 관계를 분석할 수 있습니다. 예를 들어 DevOps Guru는 테이블에서 데이터를 읽거나 쓰는 Lambda 함수의 데이터를 분석하고 연관시킬 수 있습니다. Amazon DynamoDB 이러한 방식으로 DevOps Guru는 여러 관련 리소스를 모니터링하여 이상 현상을 탐지하고 데이터베이스 솔루션에 유용한 통찰력을 제공합니다.

의 데이터베이스 작업을 모니터링합니다. Amazon DynamoDB

아래 표는 DevOps Guru가 모니터링하는 예제 시나리오와 통찰력을 보여줍니다. Amazon DynamoDB

Amazon DynamoDB 사용 사례	예제	지표
읽기 AccountProvisioned ReadCapacityUtilization 및 AccountProvisionedWriteCapacityUtilization 쓰기 요청 수가 많아서 AND가 많이 사용되는 경우를 감지합니다.	Amazon DynamoDB 읽기 또는 쓰기 요청의 테이블 소비 용량이 테이블 수준 한도에 도달했습니다.	AccountProvisioned ReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
제공된 조건 표현식이 데이터베이스의 예상과 일치하지 않아 발생하는 Amazon DynamoDB 요청의 조건부 검사 실패를 탐지합니다.	조건부 검사 실패는 테이블의 잘못된 데이터, 엄격한 조건 표현식 또는 경쟁 조건 때문에 발생합니다.	ConditionalCheckFailedRequests

에서 데이터베이스 작업을 모니터링합니다. Amazon ElastiCache

아래 표는 DevOps Guru가 모니터링하는 예제 시나리오와 통찰력을 보여줍니다. Amazon ElastiCache

DevOpsGuru가 식별한 시나리오	CloudWatch 지표 모니터링
클러스터의 수요 변화로 인해 Amazon ElastiCache 클러스터가 Redis 또는	CPU 사용률, 엔진 CPU 사용률, 제거

DevOpsGuru가 식별한 시나리오	CloudWatch 지표 모니터링
Memcached의 컴퓨팅 한도에 도달하는 시점을 감지합니다.	

CodeGuru Profiler와 통합

이 단원에서는Amazon DevOps Guru가 Amazon CodeGuru Profiler와 통합하는 방법을 간략히 살펴봅니다. CodeGuru Profiler의 권장 사항을 DevOps Guru 콘솔에서 인사이트로 확인할 수 있습니다.

Amazon DevOps Guru는 EventBridge 관리형 규칙을 사용하여 Amazon CodeGuru Profiler와 통합합니다. CodeGuru Profiler는 이벤트를 EventBridge로 전송합니다. 관리형 규칙은 기본 이벤트 버스와 함께 전송되는 이벤트를 라우팅합니다. CodeGuru Profiler의 각 인바운드 이벤트는 사전 예방적 이상 항목 보고서입니다. 더 자세한 내용은 CodeGuru Profiler를 사용한 EventBridge 활용을 참고하십시오.

DevOps Guru는 EventBridge를 통해 인바운드 이벤트를 지원합니다. 이벤트는 DevOps Guru가 식별한 권장 사항의 변경을 나타냅니다. CodeGuru Profiler는 24시간마다 하트비트 이벤트를 전송하여 이벤트의 연속성을 표시합니다. 이벤트에는 CodeGuru Profiler 권장 정보 및 컴퓨팅 리소스에 대한 메타데이터가 포함됩니다. 이벤트 라이프사이클에 대한 자세한 내용은 Amazon EventBridge 이벤트를 참고하십시오.

DevOps Guru를 설정하면 DevOps Guru는 다른 서비스의 이벤트를 라우팅하는 EventBridge 관리형 규칙을 귀하의 계정에 생성합니다. 이 규칙은 DevOps Guru로 라우팅됩니다. 알림은 인바운드 이벤트가 있을 때 전송됩니다.

이벤트 버스는 DevOps Guru 등의 소스로부터 이벤트를 수신하고 해당 이벤트 버스와 관련된 규칙으로 이를 라우팅합니다. 이벤트 버스에 대한 자세한 내용은 이벤트 버스를 참고하십시오.

일부 파라미터에 대한 자세한 내용은 Amazon EventBridge 이벤트를 참고하십시오.

DevOps Guru에서 CodeGuru Profiler 인사이트를 받으려면 다음과 같은 내용이 있어야 합니다.

- CodeGuru Profiler를 활성화해야 합니다. CodeGuru Profiler를 활성화하는 방법에 대한 자세한 내용은 CodeGuru Profiler 설정를 참고하십시오.
- DevOps Guru를 활성화해야 합니다. DevOps Guru를 활성화하는 방법에 대한 자세한 내용은 DevOps Guru 활성화를 참고하십시오.
- 동일한 리소스는 CodeGuru Profiler와 DevOps Guru 양쪽 모두에서 동일한 영역에서 모니터링되어야 합니다.

AWS 리소스를 사용한 애플리케이션 정의

Amazon DevOps Guru는 운영 인사이트를 얻기 위해 분석할 리소스를 지정하는 범위 경계에 있는 리소스를 그룹화합니다. 리소스는 AWS CloudFormation 스택의 리소스 또는 태그가 있는 리소스별로 그룹화됩니다. DevOps Guru를 설정할 때 스택이나 태그를 선택합니다. 스택이나 태그를 나중에 업데이트할 수도 있습니다. 리소스 그룹을 애플리케이션으로 생각하는 것을 권장합니다. 예를 들어, 모니터링 애플리케이션에 사용할 모든 리소스가 하나의 스택에 정의되어 있을 수 있습니다. 또는 데이터베이스 애플리케이션에서 사용하는 모든 리소스에 동일한 태그를 추가할 수도 있습니다. 이 태그는 DevOps Guru가 분석하는 리소스를 정의하는 경계입니다. 컬렉션의 모든 리소스가 이 경계 내에 있습니다. 리소스 컬렉션에 없는 계정의 모든 리소스는 경계 외부에 있으며 분석되지 않습니다. 지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOps Guru 요금을 참고하십시오.

애플리케이션의 리소스를 포함하는 범위 경계를 세 가지 방법으로 정의할 수 있습니다.

- AWS 계정 및 지역에서 지원되는 모든 AWS 리소스를 지정하십시오. 이렇게 하면 계정과 지역이 리소스 경계가 됩니다. DevOps Guru는 이 옵션을 사용하여 계정 및 지역에서 지원되는 모든 리소스를 분석합니다. 한 스택에 있는 모든 리소스는 애플리케이션으로 그룹화됩니다. 스택에 없는 모든 리소스는 자체 애플리케이션으로 그룹화됩니다.
- AWS CloudFormation 스택을 사용하여 애플리케이션의 리소스를 지정합니다. AWS CloudFormation을 사용하여 생성된 리소스가 스택에 포함됩니다. DevOps Guru에서 계정의 스택을 선택합니다. 선택한 각 스택의 리소스는 애플리케이션으로 그룹화됩니다. DevOps Guru는 스택의 모든 리소스를 분석하여 인사이트를 얻습니다.
- AWS 태그를 사용하여 애플리케이션의 리소스를 지정합니다. AWS 태그는 키와 값으로 구성됩니다. DevOps Guru에서 하나의 태그 키를 선택하고 선택적으로 해당 키와 페어를 이루는 하나 이상의 값을 선택합니다. 값을 사용하여 리소스를 애플리케이션으로 그룹화할 수 있습니다.

자세한 내용은 DevOps Guru에서 AWS 분석 지원 범위 업데이트 섹션을 참조하세요.

주제

태그를 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다.

태그를 사용하여 Amazon DevOps Guru가 분석하는 AWS 리소스를 식별하고 선택한 태그 키 및 태그 값으로 모니터링할 리소스를 그룹화할 리소스를 지정할 수 있습니다. DevOpsGuru를 설정하거나 분석된 리소스 페이지에서 분석된 리소스 편집을 선택하면 이러한 구성을 편집할 수 있습니다. 태그를 선택한 후 'devops-guru-'로 시작하는 특정 태그 키를 선택합니다. 계정의 모든 리소스를 분석하고 태그 값을 사용하여 리소스를 그룹화하려면 모든 계정 리소스를 선택합니다. 태그 값을 사용하여 DevOps Guru가 분석할 리소스를 지정하려면 특정 태그 값 선택을 선택합니다.

> **Note**
>
> 모든 계정 리소스를 선택했는데 태그 값이 없는 경우 태그 키가 없는 리소스는 그룹화되어 별도로 분석됩니다.

태그의 키를 사용하여 리소스를 식별한 다음, 해당 키가 있는 값을 사용하여 리소스를 애플리케이션으로 그룹화합니다. 예를 들어 리소스에 키를 태그한 다음`devops-guru-applications` 해당 키를 애플리케이션마다 다른 값으로 사용할 수 있습니다. 태그 키-값 페어 `devops-guru-applications/database`, `devops-guru-applications/cicd` 및 `devops-guru-applications/monitoring`를 사용해 계정에 있는 세 개의 애플리케이션을 식별할 수 있습니다. 각 애플리케이션은 동일한 태그 키-값 페어를 포함하는 관련 리소스로 구성됩니다. 리소스가 속한 AWS 서비스를 사용하여 리소스에 태그를 추가합니다. 자세한 설명은 AWS 리소스에 AWS 태그 추가 섹션을 참조하세요.

애플리케이션의 리소스에 태그를 추가한 후 이를 생성한 리소스의 태그별로 인사이트를 필터링할 수 있습니다. 태그를 사용하여 인사이트를 필터링하는 방법에 대한 자세한 내용은 DevOps Guru 인사이트 보기를 참조하십시오.

지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOps Guru 요금을 참조하십시오.

주제

AWS 태그란 무엇입니까?

태그를 사용하면 AWS 리소스를 식별하고 구성하는 데 도움이 됩니다. 많은 AWS 서비스가 태그 지정을 지원하므로 다른 서비스의 리소스에 동일한 태그를 할당하여 해당 리소스의 관련 여부를 나타낼 수 있습니다. 예를 들어, AWS Lambda 함수에 할당하는 것과 동일한 태그를 Amazon DynamoDB 테이블 리소스에 할당할 수 있습니다. 태그 사용에 대한 자세한 내용은 태그 지정 모범 사례 백서를 참조하십시오.

각 AWS 태그는 두 부분으로 구성됩니다.

- 태그 키(예: `CostCenter`, `Environment`, `Project` 또는 `Secret`). 태그 키는 대/소문자를 구분합니다.
- 태그 값(예: `111122223333`, `Production` 또는 팀 이름)으로 알려진 선택적 필드. 태그 값을 생략하는 것은 빈 문자열을 사용하는 것과 같습니다. 태그 키처럼 태그 값은 대/소문자를 구분합니다.

태그 키와 태그 값을 합해서 키-값 페어라고 합니다.

태그를 사용한 DevOps Guru 애플리케이션 정의

태그를 사용하여 Amazon DevOps Guru 애플리케이션을 정의하려면 애플리케이션을 구성하는 계정의 AWS 리소스에 해당 태그를 추가하십시오. 태그에는 키와 값이 들어 있습니다. DevOpsGuru가 분석한 각 AWS 리소스에 동일한 키를 가진 태그를 추가하는 것이 좋습니다. 태그의 다른 값을 사용하여 애플리케이션에서 리소스를 그룹화하십시오. 예를 들어 적용 범위 경계 내의 모든 `devops-guru-analysis-boundary` AWS 리소스에 키가 있는 태그를 할당할 수 있습니다. 해당 키에 다른 값을 사용하여 애플리케이션에서 계정을 식별하십시오. 세 가지 응용 프로그램에 값 `containers`, `database` 및 `monitoring`을 사용할 수 있습니다. 자세한 설명은 DevOps Guru에서 AWS 분석 지원 범위 업데이트 섹션을 참조하세요.

AWS태그를 사용하여 분석할 리소스를 지정하는 경우 키가 하나뿐인 태그를 사용할 수 있습니다. 태그의 키를 어떤 값과도 페어링할 수 있습니다. 값을 사용하여 키가 포함된 리소스를 운영 애플리케이션으로 그룹화할 수 있습니다.

> **Important**
>
> 리소스 범위를 정의하는 데 사용하는 태그의 키에 사용되는 문자열은 접두사 `Devops-guru-`로 시작해야 합니다. 태그 키는 `DevOps-Guru-deployment-application` 또는 `devops-guru-rds-application`일 수 있습니다. 키를 생성하는 경우 키의 대/소문자는 원하는 대로 선택할 수 있습니다. 키를 생성한 후에는 대/소문자를 구분합니다. 예를 들

어 DevOps Guru는 이름이 지정된 `devops-guru-rds`키와 이름이 지정된 키를 사용하는 데*`DevOps-Guru-RDS`*, 이 두 키는 서로 다른 두 개의 키로 작동합니다. 애플리케이션에서 가능한 키/값 페어는 `Devops-Guru-production-application/RDS` 또는 `Devops-Guru-production-application/containers`일 수 있습니다.

Guru에서 태그 사용하기 DevOps

Amazon DevOps Guru에서 분석할 AWS 리소스를 식별하는 AWS 태그를 지정하거나 그룹화할 리소스를 식별하는 태그 값을 지정합니다. 이러한 리소스는 리소스 적용 범위의 경계입니다. 키 하나와 0개 이상의 값을 선택할 수 있습니다.

태그를 선택하려면

1. https://console.aws.amazon.com/devops-guru/ 에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창을 연 다음 설정을 확장합니다.
3. 분석된 리소스에서 편집을 선택합니다.
4. 선택한 태그가 포함된 모든 리소스를 DevOps Guru가 분석하도록 하려면 태그를 선택하십시오. 키를 선택하고, 다음 옵션 중 하나를 선택합니다.

   - 모든 계정 리소스 - 현재 지역 및 계정의 모든 AWS 리소스를 분석합니다. 선택한 태그 키가 있는 리소스는 태그 값이 있는 경우 그 값을 기준으로 그룹화됩니다. 이 태그 키가 없는 리소스는 별도로 그룹화되고 분석됩니다.
   - 특정 태그 값 선택 - 선택한 키의 태그가 포함된 모든 리소스가 분석됩니다. DevOpsGuru는 태그 값에 따라 리소스를 애플리케이션으로 그룹화합니다.

   이 태그의 키는 `devops-guru-` 접두사로 시작해야 합니다. 이 프리픽스는 대소문자를 구분하지 않습니다. 예를 들어, 유효한 키는 `DevOps-Guru-Production-Applications`입니다.
5. 저장을 선택합니다.

AWS 리소스에 AWS 태그 추가

DevOpsGuru가 분석할 AWS 리소스를 식별하는 AWS 태그를 지정할 때는 관련 리소스가 있는 태그를 선택하십시오. 각 리소스가 속한 AWS 서비스를 사용하거나 AWS태그 편집기를 사용하여 리소스에 태그를 추가할 수 있습니다.

- 리소스 서비스를 사용하여 태그를 관리하려면 리소스가 속한 서비스의 콘솔, AWS Command Line Interface, 또는 SDK를 사용하세요. 예를 들어 Amazon Kinesis 스트림 리소스 또는 Amazon CloudFront 배포 리소스에 태그를 지정할 수 있습니다. 태그를 지정할 수 있는 리소스가 있는 두 가지 서비스 예시입니다. DevOpsGuru가 분석할 수 있는 대부분의 리소스는 태그를 지원합니다. 자세한 내용은 Amazon Kinesis 개발자 안내서의 스트림 태그 지정 및 Amazon 개발자 안내서의 배포에 태그 지정을 참조하십시오. CloudFront 다른 유형의 리소스에 태그를 추가하는 방법을 알아보려면 해당 리소스가 속한 AWS 서비스의 사용 설명서 또는 개발자 안내서를 참조하십시오.

> **Note**
>
> Amazon RDS 리소스에 태그를 지정할 때는 클러스터가 아닌 데이터베이스 인스턴스에 태그를 지정해야 합니다.

- AWS태그 편집기를 사용하여 지역 내 리소스 및 특정 AWS 서비스의 리소스별로 태그를 관리할 수 있습니다. 자세한 내용은 AWS 리소스 그룹 사용 설명서의 태그 편집기를 참조하세요.

리소스에 태그를 추가할 때 키만 추가하거나 키와 값을 추가할 수 있습니다. 예를 들어, 애플리케이션에 포함된 모든 리소스의 키를 `devops-guru-` 사용하여 태그를 생성할 수 있습니다. DevOps 키`devops-guru-`와 값RDS이 포함된 태그를 추가한 다음, 해당키-값 페어를 애플리케이션의 Amazon RDS 리소스에만 추가할 수도 있습니다. 이는 애플리케이션을 통해 Amazon RDS 리소스에서 생성된 인사이트를 콘솔에서 확인하려는 경우에만 유용합니다.

AWS CloudFormation 스택을 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다.

AWS CloudFormation 스택을 사용하여 DevOps Guru에서 분석할 AWS 리소스를 지정할 수 있습니다. 스택이란 사용자가 하나의 단위로 관리하는 AWS 리소스 모음입니다. 선택한 스택의 리소스가 DevOps Guru 적용 범위 경계를 구성합니다. 선택한 각 스택에 대해 지원되는 리소스의 운영 데이터를 분석하여 이상 동작이 있는지 확인합니다. 그런 다음 이러한 문제를 관련 이상 현상으로 그룹화하여 인사이트를 확보합니다. 각 인사이트에는 문제를 해결하는 데 도움이 되는 하나 이상의 권장 사항이 포함되어 있습니다. 지정할 수 있는 스택 개수는 최대 1000개입니다. 자세한 내용을 알아보려면 AWS CloudFormation 사용 설명서 및 DevOps Guru에서 AWS 분석 지원 범위 업데이트에서 스택 작업을 참조하세요.

스택을 선택하면 DevOps Guru는 스택에 추가한 모든 리소스를 즉시 분석하기 시작합니다. 스택에서 리소스를 제거하면 해당 리소스는 더 이상 분석되지 않습니다.

DevOps Guru가 계정에서 지원되는 모든 리소스를 분석하도록 선택하면 (즉, AWS 계정과 지역이 DevOps Guru 적용 범위 경계임) DevOps Guru는 스택에 있는 리소스를 포함하여 계정에서 지원되는 모든 리소스를 분석하고 인사이트를 생성합니다. 스택에 없는 리소스의 이상 현상으로 생성된 인사이트는 계정 수준에서 그룹화됩니다. 스택에 있는 리소스의 이상 징후로부터 인사이트를 생성한 경우 스택 수준에서 그룹화됩니다. 자세한 내용은 이상 동작이 인사이트로 그룹화되는 방식 이해하기 섹션을 참조하세요.

DevOps Guru가 분석할 스택 선택

리소스를 생성하는 AWS CloudFormation 스택을 선택하여 Amazon DevOps Guru에서 분석할 리소스를 지정합니다. 이를 위해 AWS Management Console 또는 SDK를 사용할 수 있습니다.

주제

- DevOps Guru가 분석할 스택 선택(콘솔)
- DevOps Guru가 분석할 스택 선택(DevOps Guru SDK)

DevOps Guru가 분석할 스택 선택(콘솔)

콘솔을 사용하여 AWS CloudFormation 스택을 추가할 수 있습니다.

분석할 리소스가 포함된 스택을 선택하려면

1. https://console.aws.amazon.com/devops-guru/에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. DevOps Guru 분석 범위에서 관리를 선택합니다.
4. 선택한 스택에 있는 리소스를 DevOps Guru가 분석하도록 하려면 CloudFormation 스택을 선택하고 다음 옵션 중 하나를 선택하십시오.
   - 모든 리소스 - 계정의 스택에 있는 모든 리소스가 분석됩니다. 각 스택의 리소스는 자체 애플리케이션으로 그룹화됩니다. 스택에 없는 계정 내 리소스는 분석되지 않습니다.
   - 스택 선택 - DevOps Guru가 분석할 스택을 선택합니다. 선택한 각 스택의 리소스는 자체 애플리케이션으로 그룹화됩니다. 스택 찾기에서 스택 이름을 입력하여 특정 스택을 빠르게 찾을 수 있습니다. 최대 1,000개의 스택을 선택할 수 있습니다.
5. Save를 선택합니다.

DevOps Guru가 분석할 스택 선택(DevOps Guru SDK)

Amazon DevOps Guru SDK를 사용하여 AWS CloudFormation 스택을 지정하려면 `UpdateResourceCollection` 방법을 사용하십시오. 자세한 내용은 Amazon DevOps Guru API 참조의 UpdateResourceCollection을 참조하십시오.

아마존과의 협력 EventBridge

Amazon DevOps Guru는 Amazon과 통합되어 통찰력과 관련된 특정 이벤트 및 해당 통찰력 업데이트를 알려줍니다. EventBridge AWS 서비스의 이벤트는 거의 EventBridge 실시간으로 전달됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 태스크를 지정할 수 있습니다. 자동으로 트리거할 수 있는 작업은 다음과 같습니다.

- 함수 호출 AWS Lambda
- Amazon Elastic Compute Cloud 실행 명령 호출
- Amazon Kinesis Data Streams로 이벤트 릴레이
- Step Functions 상태 머신 활성화
- Amazon SNS 또는 Amazon SQS 알림

다음과 같은 사전 정의된 패턴을 선택하여 이벤트를 필터링하거나 사용자 지정 패턴 규칙을 생성하여 지원되는 리소스에서 작업을 시작할 수 있습니다. AWS

- DevOps 구루: 뉴 인사이트 오픈
- DevOps 구루 뉴 어노멀리 어소시에이션
- DevOps 구루 인사이트 심각도 업그레이드
- DevOps Guru 새 권장 사항 생성
- DevOps 구루 인사이트 폐점

전문가를 위한 DevOps 이벤트

다음은 DevOps Guru의 이벤트 예시입니다. 이벤트는 최선의 작업에 근거하여 발생됩니다. 이벤트 패턴에 대해 자세히 알아보려면 Amazon EventBridge 또는 Amazon EventBridge 이벤트 패턴 시작하기를 참조하십시오.

DevOpsGuru뉴 인사이트 오픈 이벤트

DevOps Guru는 새 인사이트를 열면 다음 이벤트를 보냅니다.

```
{
    "version" : "0",
    "id" : "08108845-ef90-00b8-1ad6-2ee5570ac6c4",
    "detail-type" : "DevOps Guru New Insight Open",
```

```
    "source" : "aws.devops-guru",
    "account" : "123456789012",
    "time" : "2021-11-01T17:06:10Z",
    "region" : "us-east-1",
    "resources" : [ ],
    "detail" : {
      "insightSeverity" : "high",
      "insightDescription" : "ApiGateway 5XXError Anomalous In Stack TestStack",
      "insightType" : "REACTIVE",
      "anomalies" : [
        {
          "startTime" : "1635786000000",
          "id" : "AL41JDFFQPYlZlXD8cpREkAAAAF83HGGgC9TmTr9lbfJ7sCiISlWMeFCbHY_XXXX",
          "sourceDetails" : [
            {
              "dataSource" : "CW_METRICS",
              "dataIdentifiers" : {
                "period" : "60",
                "stat" : "Average",
                "unit" : "None",
                "name" : "5XXError",
                "namespace" : "AWS/ApiGateway",
                "dimensions" : [
                  {
                    "name" : "ApiName",
                    "value" : "Test API Service"
                  },
                  {
                    "name" : "Stage",
                    "value" : "prod"
                  }
                ]
              }
            }
          ]
        }
      ],
      "accountId" : "123456789012",
      "messageType" : "NEW_INSIGHT",
      "insightUrl" : "https://us-east-1.console.aws.amazon.com/devops-guru/#/insight/
reactive/AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "startTime" : "1635786120000",
      "insightId" : "AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "region" : "us-east-1"
```

```
    }
  },
```

심각도가 높은 새 인사이트를 위한 사용자 지정 예시 이벤트 패턴

규칙은 이벤트 패턴을 사용하여 이벤트를 선택하고 대상으로 이를 라우팅합니다. 다음은 샘플 DevOps Guru 이벤트 패턴입니다.

```
{
  "source": [
    "aws.devops-guru"
  ],
  "detail-type": [
    "DevOps Guru New Insight Open"
  ],
  "detail": {
    "insightSeverity": [
         "high"
         ]
  }
}
```

DevOps Guru 설정 업데이트

다음과 같은 Amazon DevOps Guru 설정을 업데이트할 수 있습니다.

- DevOps Guru 지원 범위 이 항목에서 귀하의 계정에 있는 리소스 중 어떤 리소스를 분석할지 정합니다.
- 내 알림입니다. 이 항목에서 중요한 DevOps Guru 이벤트에 대한 알림을 받는 데 사용되는 Amazon Simple Notification Service 주제를 정합니다.
- 향상된 인사이트를 위한 기능 여기에는 로그 이상 감지, 암호화, AWS Systems Manager 통합 설정이 포함됩니다. 이 항목에서 DevOps Guru에서 로그 데이터를 표시할지 여부, 추가 보안 키를 사용할지 여부, 새로운 각 인사이트에 대해 Systems Manager OpsCenter에서 OpsItem을 생성할지 여부를 정합니다.

주제

관리 계정 설정 업데이트

조직에 있는 계정에 대해 DevOps Guru를 구성할 수 있습니다. 위임된 관리자를 등록하지 않은 경우 위임된 관리자 등록을 선택하여 등록할 수 있습니다. 자세한 내용은 개발자 안내서의 위임된DevOps Guru 활성화를 참조하세요.

DevOps Guru에서 AWS 분석 지원 범위 업데이트

귀하의 계정에 있는 AWS 리소스 중 DevOps Guru가 어떤 리소스를 분석할지에 대한 내용을 업데이트할 수 있습니다. 이 항목을 업데이트하려면 콘솔에서 분석된 리소스 페이지로 이동한 다음 편집을 선택합니다. 자세한 내용은 분석한 리소스 보기 섹션을 참조하세요.

DevOps Guru에서 알림 업데이트

중요한 Amazon DevOps Guru 이벤트에 대한 알림을 받기 위해 사용되는 Amazon Simple Notification Service 주제를 설정합니다. 귀하의 AWS 계정에 이미 있는 주제 이름의 목록에서 선택하거나, DevOps Guru가 귀하의 계정에 생성하는 새 주제의 이름을 입력하거나, 귀하의 지역 내 모든 AWS 계정에 있는 기존 주제의 Amazon 리소스 이름(ARN)을 입력할 수 있습니다. 귀하의 계정에 없는 주제의 ARN을 지정하려면, IAM 정책을 추가하여 DevOps Guru가 해당 주제에 액세스할 수 있는 권한을 부여해야 합니다. 자세한 내용은 Amazon SNS 주제에 대한 권한 섹션을 참조하세요. 최대 두 개의 주제를 지정할 수 있습니다.

DevOps Guru는 다음과 같은 업데이트에 대해 알림을 보냅니다.

- 새로운 인사이트가 생성됩니다.
- 새로운 이상 항목이 인사이트에 추가됩니다.
- 인사이트의 심각도가 `Low` 또는 `Medium`에서 `High`(으)로 업그레이드됩니다.
- 인사이트 상태가 진행 중에서 해결됨으로 바뀝니다.
- 인사이트에 대한 권장 사항이 파악됩니다.

또한, DevOps Guru는 귀하가 DevOps Guru 계정에 리소스를 추가하려고 할 때 선택한 AWS CloudFormation 스택 또는 태그 키가 유효하지 않으면 알림을 보냅니다.

문제에 대한 모든 종류의 업데이트에 대해 Amazon SNS 알림을 수신하거나, 문제가 개시, 종결, 심각도가 변경될 때만 Amazon SNS 알림을 수신하도록 선택할 수 있습니다. 기본 설정으로는 모든 업데이트에 대한 알림을 받습니다.

알림을 업데이트하려면 먼저 알림 페이지로 이동한 다음 Amazon SNS 알림 주제에 대한 구성을 추가, 제거 또는 업데이트할지 여부를 선택합니다.

주제

DevOps Guru 콘솔에서 알림 설정으로 이동합니다.

알림을 업데이트하려면 먼저 알림 설정 섹션으로 이동해야 합니다.

알림 설정 섹션으로 이동하려면,

1. https://console.aws.amazon.com/devops-guru/에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.

   설정 페이지에는 구성된 Amazon SNS 주제에 대한 정보가 있는 알림 섹션이 포함되어 있습니다.

DevOps Guru 콘솔에 Amazon SNS 알림 주제 추가

DevOps Guru 콘솔에 Amazon SNS 알림 주제를 추가하려면,

1. the section called “DevOps Guru 콘솔에서 알림 설정으로 이동합니다.”.
2. 알림 추가를 선택합니다.
3. Amazon SNS 주제를 추가하려면 다음 중 하나를 수행합니다.
   - 이메일을 사용하여 새 SNS 주제 생성을 선택합니다. 그런 후에 이메일 주소 지정에서 알림을 받으려는 이메일 주소를 입력합니다. 추가 이메일 주소를 입력하려면 새 이메일 추가를 선택합니다.
   - 기존 SNS 주제 사용을 선택합니다. 그런 후에 귀하의 AWS 계정에 있는 주제 선택에서 사용하려는 주제를 선택합니다.
   - 기존의 SNS 주제 ARN을 선택하여 다른 계정의 기존 주제 지정을 선택합니다. 그런 후에 주제의 ARN 입력에서 주제 ARN을 입력합니다. ARN은 주제에 대한 Amazon 리소스 이름(ARN)입니다. 다른 계정에서 주제를 지정할 수도 있습니다. 다른 계정에서 주제를 사용하는 경우 주제에 리소스 정책을 추가해야 합니다. 자세한 내용은 Amazon SNS 주제에 대한 권한 섹션을 참조하세요.
4. 저장을 선택합니다.

DevOps Guru 콘솔에서 Amazon SNS 알림 주제 제거

DevOps Guru 콘솔에서 Amazon SNS 주제를 제거하려면,

1. the section called “DevOps Guru 콘솔에서 알림 설정으로 이동합니다.”.
2. 기존 주제 선택을 선택합니다.

3. 드롭다운 메뉴에서 제거하려는 주제를 선택합니다.
4. [Remove]를 선택합니다.
5. 저장을 선택합니다.

Amazon SNS 알림 구성 업데이트

DevOps Guru에는 Amazon SNS 알림 주제에 대해 두 가지 유형의 알림 구성이 있습니다. 모든 심각도 수준에 대해 알림을 수신하거나 높은 심각도와 중간 심각도의 알림만 수신하도록 선택할 수 있습니다. 또한, 모든 종류의 업데이트에 대해 알림을 받거나 일부 업데이트 종류에 대해서만 알림을 받도록 선택할 수 있습니다.

문제에 관련된 모든 종류의 업데이트에 대해 Amazon SNS 알림을 수신하기로 선택하면 DevOps Guru는 다음과 같은 업데이트에 대해 알림을 보냅니다.

- 새로운 인사이트가 생성됩니다.
- 새로운 이상 항목이 인사이트에 추가됩니다.
- 인사이트의 심각도가 `Low` 또는 `Medium`에서 `High`(으)로 업그레이드됩니다.
- 인사이트 상태가 진행 중에서 해결됨으로 바뀝니다.
- 인사이트에 대한 권장 사항이 파악됩니다.

기본 설정으로는 높은 심각도와 중간 심각도 수준의 알림만 수신하고 모든 종류의 업데이트에 대한 알림을 받습니다.

Amazon SNS 알림 주제에 대한 알림 구성을 업데이트하려면,

1. the section called “DevOps Guru 콘솔에서 알림 설정으로 이동합니다.”.
2. 기존 주제 선택을 선택합니다.
3. 드롭다운 메뉴에서 업데이트하려는 주제를 선택합니다.
4. 모든 심각도 수준을 선택하여 심각도가 [높음], [중간], [낮음] 수준일 때 알림을 받거나 높음 및 중간만을 선택하여 심각도가 높거나 중간 수준일 때 알림을 받을 수 있습니다.
5. 인사이트와 관련된 모든 업데이트에 대해 알림 받기 또는 인사이트가 개시되거나, 종료되거나, 심각도가 낮음 또는 보통에서 높음으로 변경될 때 알림 받기를 선택합니다.
6. 저장을 선택합니다.

Amazon SNS 주제로 권한 추가됨

Amazon SNS 주제는 AWS Identity and Access Management (IAM) 리소스 정책을 포함하는 리소스입니다. 여기서 주제를 지정하면 DevOps Guru는 해당 리소스 정책에 다음과 같은 권한을 추가합니다.

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

DevOps Guru가주제를 사용하여 알림을 게시하려면 이러한 권한이 필요합니다. 해당 주제에 대해 이러한 권한을 갖고 싶지 않다면 해당 권한을 안전하게 제거할 수 있습니다. 그러면 해당 주제를 선택하기 전과 동일하게 계속 작동합니다. 하지만, 이렇게 추가된 권한을 제거하면 DevOps Guru는 이 주제를 사용하여 알림을 생성할 수 없습니다.

DevOps Guru 알림 필터링

the section called “Amazon SNS 알림 구성 업데이트” 또는 Amazon SNS 구독 필터 정책을 사용하여 DevOps Guru 알림을 필터링할 수 있습니다.

주제

Amazon SNS 구독 필터 정책을 사용한 알림 필터링

Amazon Simple Notification Service(Amazon SNS) 구독 필터 정책을 생성하여 Amazon DevOps Guru 로부터 받는 알림 수를 줄일 수 있습니다.

필터 정책을 사용하여 수신하는 알림 유형을 지정합니다. 다음과 같은 키워드를 사용하여 Amazon SNS 메시지를 필터링할 수 있습니다.

- `NEW_INSIGHT` — 새로운 인사이트가 생성되면 알림을 받습니다.
- `CLOSED_INSIGHT` — 기존 인사이트가 닫히면 알림을 받습니다.
- `NEW_RECOMMENDATION` — 인사이트에서 새로운 권장 사항이 생성되면 알림을 받습니다.
- `NEW_ASSOCIATION` — 인사이트에서 새로운 이상 항목이 감지되면 알림을 받습니다.
- `CLOSED_ASSOCIATION` — 기존의 이상 항목이 종료되면 알림을 받습니다.
- `SEVERITY_UPGRADED` — 인사이트의 심각도가 업그레이드되면 알림을 받습니다.

주제 구독 방법에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 주제 구독 필터 정책을 참조하세요. 필터 정책에서 해당 정책의 `MessageType`(이)가 포함된 키워드 중 하나를 지정합니다. 예를 들어, Amazon SNS 주제가 인사이트에서 새로운 이상 항목을 감지할 때만 알림을 전송하도록 지정하는 필터에는 다음과 같은 내용이 표시됩니다.

```
{
  "MessageType":["NEW_ ASSOCIATION"]
}
```

Amazon DevOps Guru에 대한 Amazon SNS 알림 필터링된 예

다음은 필터 정책이 있는 Amazon SNS 주제의 Amazon Simple Notification Service(Amazon SNS) 알림에 대한 예입니다. `MessageType`이(가) `NEW_ASSOCIATION`(으)로 설정되어 있으므로 인사이트에서 새로운 이상 항목이 감지될 때만 알림을 보냅니다.

```
{
      "accountId": "123456789012",
      "region": "us-east-1",
      "messageType": "NEW_ASSOCIATION",
      "insightId": "ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-Function duration due to increased number of invocations",
```

```
      "insightUrl": "https://us-east-1.console.aws.amazon.com/devops-guru/insight/
reactive/ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightType": "REACTIVE",
      "insightDescription": "At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-Function had\n an increased duration anomaly possibly caused by
 the Lambda function invocation increase. DevOps Guru has detected this is a repeated
 insight. DevOps Guru treats repeated insights as 'Low Severity'.",
      "startTime": 1628767500000,
      "startTimeISO": "2023-03-29T22:00:00Z",
      "anomalies": [
        {
          "id": "AG2n8ljW74BoI1CHu-m_oAgAAAF7Ohu24N4Yro69ZSdUtn_alzPH7VTpaL30JXiF",
          "startTime": 1628767500000,
          "startTimeISO": "2023-03-29T22:00:00Z",
          "openTime": 1680127740000,
          "openTimeISO": "2023-03-29T22:09:00Z",
          "sourceDetails": [
            {
              "dataSource": "CW_METRICS",
              "dataIdentifiers": {
                "namespace": "AWS/SQS",
                "name": "ApproximateAgeOfOldestMessage",
                "stat": "Maximum",
                "unit": "None",
                "period": "60",
                "dimensions": "{\"QueueName\":\"FindingNotificationsDLQ\"}"
              }
            }
          ],
          "associatedResourceArns":[
           "arn:aws:sns:us-east-1:123456789012:DevOpsGuru-insights-sns"
          ]
        }
      ],
      "resourceCollection":{
      "cloudFormation":{
         "stackNames":[
            "CapstoneNotificationPublisherEcsApplicationInfrastructure"
          ]
        }
      }
}
```

DevOps Guru에서 AWS Systems Manager 통합 업데이트

AWS Systems Manager OpsCenter에서 새로운 각 인사이트에 대해 OpsItem 생성을 활성화할 수 있습니다. OpsCenter는 운영 작업 항목(OpsItem)을 보고, 조사하고, 검토할 수 있는 중앙 집중식 시스템입니다. 인사이트에 대한 OpsItems는 각 인사이트 생성을 촉발시킨 이례적인 행동을 해결하는 작업을 관리하는 데 도움이 될 수 있습니다. 자세한 내용은 AWS Systems Manager사용자 가이드의 AWS Systems ManagerOpsCenter 및 OpsItem으로 작업을 참조하세요.

> **Note**
>
> OpsItem의 태그 필드 키 또는 값을 변경하면 DevOps Guru가 해당 OpsItem을 업데이트할 수 없습니다. 예를 들어, OpsItem의 태그를 `"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"`에서 다른 것으로 변경하는 경우 DevOps Guru는 해당 OpsItem을 업데이트할 수 없습니다.

Systems Manager 통합을 관리하려면,

1. https://console.aws.amazon.com/devops-guru/에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. AWS Systems Manager통합에서 DevOps Guru를 활성화하여 각 인사이트에 대해 OpsCenter에서 AWS OpsItem 생성을 선택하여 새로운 각각의 인사이트에 대해 OpsItem을 생성하도록 합니다. 새로운 각각의 인사이트에 대해 OpsItem이 생성되는 것을 중지하려면 선택을 취소하십시오.

계정에서 생성된 OpsItem에 대한 요금이 청구됩니다. 자세한 내용은 AWS Systems Manager 요금을 참조하세요.

DevOps Guru에서 로그 이상 감지 업데이트

로그 이상 감지 설정을 관리하려면,

1. https://console.aws.amazon.com/devops-guru/에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 로그 이상 감지에서 로그 이상 감지를 활성화하여 DevOps Guru에 권한을 부여함으로써 DevOps Guru가 인사이트와 관련된 로그 데이터를 표시를 선택하여 DevOps Guru가 인사이트와 관련된 로그 데이터를 표시할 수 있도록 합니다.

DevOps Guru에서 암호화 설정 업데이트

AWS 소유형 키 또는 AWS KMS 고객 관리형 키를 사용하도록 암호화 설정을 업데이트할 수 있습니다. 기존 고객 관리형 AWS KMS 키에서 새로운 고객 관리형 AWS KMS 키로 전환하면 DevOps Guru는 새 키를 사용하여 새로 수집된 메타데이터를 자동으로 암호화하기 시작합니다. 이전 데이터는 이전에 구성된 고객 관리형 AWS KMS 키로 암호화된 상태로 유지됩니다.

> **Note**
>
> 권한 부여를 취소하거나, 이전의 AWS KMS 키를 비활성화 또는 삭제하면 DevOps Guru는 이 키로 암호화된 모든 데이터에 액세스할 수 없게 되며 읽기 작업을 수행할 때 `AccessDeniedException`이(가) 표시될 수 있습니다.

암호화 설정을 관리하려면,

1. https://console.aws.amazon.com/devops-guru/에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 암호화 섹션에서 암호화 편집을 선택합니다.
4. 데이터를 보호하는 데 사용할 암호화 유형을 선택합니다. 기본 AWS 소유형 키를 사용하거나, 기존의 고객 관리형 키를 선택하거나, 새로운 고객 관리형 AWS KMS 키를 생성할 수 있습니다.
5. 저장을 선택합니다.

암호화는 DevOps Guru 보안의 중요한 부분입니다. 자세한 내용은 the section called “데이터 보호” 섹션을 참조하세요.

알림 보기

Guru에는 다양한 유형의 알림이 있습니다. DevOps

주제

이 페이지에 있는 단원에서는 각 알림 유형의 예를 보여드립니다.

새로운 인사이트

새로운 인사이트에 대한 알림에는 다음과 같은 정보가 포함됩니다.

```
{
   "accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-4",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"DevOps Guru has detected this is a repeated insight. DevOps
 Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680148920000,
   "startTimeISO": "2023-03-30T04:02:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime": 1680148800000,
         "startTimeISO": "2023-03-30T04:00:00Z",
```

```
         "openTime": 1680148920000,
         "openTimeISO": "2023-03-30T04:02:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
                  "name":"ApproximateAgeOfOldestMessage",
                  "namespace":"AWS/SQS",
                  "period":"60",
                  "stat":"Maximum",
                  "unit":"None",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        },
   }
}
```

종결된 인사이트

종결된 인사이트에 대한 알림에는 다음과 같은 정보가 포함됩니다.

```
{
"accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"CLOSED_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "DynamoDB table writes are under utilized in mock-stack",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription":"DynamoDB table writes are under utilized",
```

```
    "insightSeverity":"medium",
    "startTime": 1670612400000,
    "startTimeISO": "2022-12-09T19:00:00Z",
    "endTime": 1679994000000,
    "endTimeISO": "2023-03-28T09:00:00Z",
    "anomalies":[
       {
          "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
          "startTime": 1665428400000,
          "startTimeISO": "2022-10-10T19:00:00Z",
          "endTime": 1679986800000,
          "endTimeISO": "2023-03-28T07:00:00Z",
          "openTime": 1670612400000,
          "openTimeISO": "2022-12-09T19:00:00Z",
          "closeTime": 1679994000000,
          "closeTimeISO": "2023-03-28T09:00:00Z",
          "description":"Empty receives while messages are available",
          "anomalyResources":[
             {
                "type":"AWS::SQS::Queue",
                "name":"SampleQueue"
             }
          ],
          "sourceDetails":[
             {
                "dataSource":"CW_METRICS",
                "dataIdentifiers":{
                "name":"NumberOfEmptyReceives",
                   "namespace":"AWS/SQS",
                   "period":"60",
                   "stat":"Sum",
                   "unit":"COUNT",
                   "dimensions":"{\"QueueName\":\"SampleQueue\"}"
                }
             }
          ],
         "associatedResourceArn": [
             "arn:aws:sqs:us-east-1:123456789101:SampleQueue"
         ]
       }
    ],
    "resourceCollection":{
         "cloudFormation":{
             "stackNames":[
```

```
                "SampleApplication"
            ]
        }
    }
}
```

새 연결

새 연결에 대한 알림에는 다음과 같은 정보가 포함됩니다.

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_ASSOCIATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-GetOneFunction duration due to increased number of
 invocations",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-GetOneFunction had\nan increased duration anomaly possibly
 caused by the Lambda function invocation increase. DevOps Guru has detected this is a
 repeated insight. DevOps Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680127200000,
   "startTimeISO": "2023-03-29T22:00:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime":1672945500000,
         "startTimeISO": "2023-03-29T22:00:00Z",
         "openTime": 1680127740000,
         "openTimeISO": "2023-03-29T22:09:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
               "namespace":"AWS/SQS",
                  "name":"ApproximateAgeOfOldestMessage",
                  "stat":"Maximum",
                  "unit":"None",
```

```
                  "period":"60",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

신규 권장 사항

새 권장 사항에 대한 알림에는 다음과 같은 정보가 포함됩니다.

```
{
   "accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"NEW_RECOMMENDATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "Recreation of AWS SDK Service Clients",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription": "Usually for a given service you can create one [AWS SDK
 service client](https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/creating-
clients.html) and reuse that client across your entire service.\n\nWhen instead you
 create a new AWS SDK service client for each call (e.g. for DynamoDB) it\u0027s
 generally a waste of CPU time.",
   "insightSeverity":"medium",
   "startTime": 1680125893576,
   "startTimeISO": "2023-03-29T21:38:13.576Z",
   "recommendations":[
      {
         "name":"Tune Availability Zones of your Lambda Function",
```

```
        "description":"Based on your configurations, we recommend that you set
 SampleFunction to be deployed in at least 3 Availability Zones to maintain Multi
 Availability Zone Redundancy.",
        "reason":"Lambda Function SampleFunction is currently only deployed to 2
 unique Availability zones in a region with 7 total Availability zones.",
        "link":"https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html",
        "relatedAnomalies":[
           {
              "sourceDetails":{
                   "cloudWatchMetrics":null
              },
              "resources":[
                 {
                    "name":"SampleFunction",
                    "type":"AWS::Lambda::Function"
                 }
              ],
              "associatedResourceArns": [
                 "arn:aws:lambda:arn:123456789101:SampleFunction"
              ]
           }
        ]
     }
  ],
  "resourceCollection": {
       "cloudFormation": {
       "stackNames":[
           "SampleApplication"
        ]
     }
  }
}
```

심각도 업그레이드됨

심각도 업그레이드에 대한 알림에는 다음과 같은 정보가 포함됩니다.

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"SEVERITY_UPGRADED",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-11",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
   "insightType":"REACTIVE",
   "insightDescription": "DevOps Guru has detected this is a repeated insight. DevOps
 Guru will treat future occurrences of this insight as 'Low Severity' for the next 7
 days.",
   "insightSeverity":"high",
   "startTime": 1680127320000,
   "startTimeISO": "2023-03-29T22:02:00Z",
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

리소스 검증 실패

AWS CloudFormation스택과 AWS 태그를 사용하여 DevOps Guru가 분석할 AWS 리소스를 필터링하고 식별할 수 있습니다. Guru가 리소스를 식별하는 데 사용할 잘못된 스택이나 태그를 선택하면 DevOps Guru가 알림을 DevOps 생성합니다. `SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE` 이는 지정한 태그 또는 스택 이름에 관련 리소스가 없는 경우 발생할 수 있습니다. DevOpsGuru 필터링 방법을 최대한 활용하려면 관련 리소스가 있는 스택과 태그를 선택하십시오.

```
{
    "accountId":"123456789101",
    "region":"eu-west-1",
    "messageType":"SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE",
    "ResourceFilterType": "Tags",
    "InvalidResourceNames": [
         "Devops-Guru-tag-key-tag-value"
    ],
    "awsInsightSource": "aws.devopsguru"
}
```

DevOps Guru가 분석한 리소스 보기

DevOps Guru는 `ListMonitoredResources` 작업을 사용하여 분석 중인 리소스 이름 및 애플리케이션 경계 목록을 제공합니다. 이 정보는 Amazon CloudWatch, AWS CloudTrail 및 DevOps 전문가 서비스 연결 역할을 사용하는 기타 AWS 서비스에서 수집됩니다.

AWS Lambda, 또는 Amazon RDS와 같은 다른 서비스의 API에 액세스할 수 있는 명시적인 권한이 사용자에게 없더라도 DevOps Guru는 `ListMonitoredResources` 작업이 허용되는 한 해당 서비스의 리소스 목록을 계속 제공합니다.

주제

DevOps Guru에서 AWS 분석 지원 범위 업데이트

귀하의 계정에 있는 AWS 리소스 중 DevOps Guru가 어떤 리소스를 분석할지에 대한 내용을 업데이트할 수 있습니다. 분석된 리소스는 DevOps Guru 적용 범위를 구성합니다. 경계를 지정하면 리소스가 애플리케이션별로 그룹화됩니다. 네 가지 경계 적용 범위 옵션이 있습니다.

- DevOps Guru는 계정에 지원되는 모든 리소스를 분석합니다. 스택에 있는 계정의 모든 리소스는 애플리케이션으로 그룹화됩니다. 계정에 스택이 여러 개 있는 경우 각 스택의 리소스가 자체 애플리케이션을 구성합니다. 계정의 리소스가 스택에 없는 경우 해당 리소스는 자체 애플리케이션으로 그룹화됩니다.
- 리소스를 정의하는 AWS CloudFormation 스택을 선택하여 리소스를 지정하세요. 이렇게 하면 DevOps Guru가 선택한 스택에 지정된 모든 리소스를 분석합니다. 계정의 리소스가 선택한 스택으로 정의되지 않은 경우 해당 리소스는 분석되지 않습니다. 자세한 내용을 알아보려면 AWS CloudFormation 사용 설명서 및 DevOpsGuru에 대한 적용 범위 결정에서 스택 작업을 참조하세요.
- AWS 태그를 사용하여 리소스를 지정합니다. DevOps Guru는 계정 및 지역의 모든 리소스 또는 선택한 태그 키가 포함된 모든 리소스를 분석합니다. 리소스는 선택한 태그 값을 기준으로 그룹화됩니다. 자세한 내용은 태그를 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다. 섹션을 참조하세요.
- 리소스를 분석하지 않도록 지정하여 리소스 분석으로 인한 요금 발생을 멈추세요.

> **Note**
>
> 적용 범위를 업데이트하여 리소스 분석을 중단하는 경우, 과거 DevOps Guru에서 생성한 기존 인사이트를 계속 검토하면 소액의 요금이 부과될 수 있습니다. 이러한 요금은 인사이트 정보를 검색하고 표시하는 데 사용되는 API 호출과 관련이 있습니다. 자세한 정보는 Amazon DevOps Guru 요금을 참조하세요.

DevOps Guru는 지원되는 서비스와 관련된 모든 리소스를 지원합니다. 지원되는 서비스 및 리소스에 대한 자세한 내용은 Amazon DevOps Guru 요금을 참고하십시오.

DevOps Guru 분석 범위를 관리하려면

1. https://console.aws.amazon.com/devops-guru/에서 Amazon DevOps Guru 콘솔을 엽니다.
2. 탐색 창에서 분석된 리소스를 확장하십시오.
3. 편집(Edit)을 선택합니다.
4. 다음 커버리지 옵션 중 하나를 선택합니다.

   - DevOps Guru가 AWS 계정 및 리전에서 지원되는 모든 리소스를 분석하도록 하려면 모든 계정 리소스를 선택합니다. 이 옵션을 선택하면 AWS 계정이 리소스 분석 적용 범위의 경계가 됩니다. 계정의 각 스택에 있는 모든 리소스는 자체 애플리케이션으로 그룹화됩니다. 스택에 없는 나머지 리소스는 모두 자체 애플리케이션으로 그룹화됩니다.
   - 선택한 스택에 있는 리소스를 DevOps Guru가 분석하도록 하려면 CloudFormation 스택을 선택하고 다음 옵션 중 하나를 선택하십시오.
     - 모든 리소스 - 계정의 스택에 있는 모든 리소스가 분석됩니다. 각 스택의 리소스는 자체 애플리케이션으로 그룹화됩니다. 스택에 없는 계정 내 리소스는 분석되지 않습니다.
     - 스택 선택 - DevOps Guru가 분석할 스택을 선택합니다. 선택한 각 스택의 리소스는 자체 애플리케이션으로 그룹화됩니다. 스택 찾기에서 스택 이름을 입력하여 특정 스택을 빠르게 찾을 수 있습니다. 최대 1,000개의 스택을 선택할 수 있습니다.

     자세한 내용은 AWS CloudFormation 스택을 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다. 섹션을 참조하세요.
   - 선택한 태그가 포함된 모든 리소스를 DevOps Guru가 분석하도록 하려면 태그를 선택합니다. 키를 선택하고, 다음 옵션 중 하나를 선택합니다.

- 모든 계정 리소스 — 현재 리전 및 계정의 모든 AWS 리소스를 분석합니다. 선택한 태그 키가 있는 리소스는 태그 값이 있는 경우 그 값을 기준으로 그룹화됩니다. 이 태그 키가 없는 리소스는 별도로 그룹화되고 분석됩니다.
- 특정 태그 값 선택 - 선택한 키와 함께 태그가 포함된 모든 리소스가 분석됩니다. DevOps Guru는 태그 값을 기준으로 리소스를 애플리케이션으로 그룹화합니다.

이 태그의 키는 `devops-guru-` 접두사로 시작해야 합니다. 이 프리픽스는 대소문자를 구분하지 않습니다. 예를 들어, 유효한 키는 `DevOps-Guru-Production-Applications`입니다. 자세한 내용은 태그를 사용하여 DevOps Guru 애플리케이션의 리소스를 식별합니다. 섹션을 참조하세요.

- DevOps Guru가 리소스를 분석하지 않도록 하려면 없음을 선택합니다. 이 옵션은 DevOps Guru를 비활성화하여 리소스 분석으로 인한 요금이 발생하지 않도록 합니다.

5. Save를 선택합니다.

사용자에 대한 분석 리소스 보기 제거

Lambda 또는 Amazon RDS와 같은 다른 서비스의 API에 액세스할 수 있는 명시적인 권한이 사용자에게 없더라도 DevOps Guru는 `ListMonitoredResources` 작업이 허용되는 한 해당 서비스의 리소스 목록을 계속 제공합니다. 이 동작을 변경하려면 AWS IAM 정책을 업데이트하여 이 작업을 거부할 수 있습니다.

```
{
            "Sid": "DenyListMonitoredResources",
            "Effect": "Deny",
            "Action": [
                "devops-guru:ListMonitoredResources"
            ]
}
```

DevOps Guru 모범 사례

다음과 같은 모범 사례를 통해 Amazon DevOps Guru에서 감지한 비정상적인 동작을 이해하고 진단 및 해결할 수 있습니다. DevOps Guru 콘솔에서 인사이트 이해하기(으)로 모범 사례를 사용하여 DevOps Guru에서 감지한 운영 문제를 해결해 보십시오.

- 인사이트의 타임라인 뷰에서 강조 표시된 지표를 먼저 살펴보십시오. 이러한 지표는 문제의 주요 지표인 경우가 많습니다.
- Amazon CloudWatch를 사용하면 인사이트에서 첫 번째로 강조 표시된 지표 바로 전에 발생한 지표를 보고 동작이 언제 어떻게 변했는지 정확히 찾아낼 수 있습니다. 이걸로 문제를 진단하고 해결하는 데 도움을 받을 수 있습니다.
- Amazon RDS 리소스의 경우 Performance Insights 지표를 살펴보십시오. 카운터 지표와 데이터베이스 부하를 상호 연관시켜 성능 문제에 대한 자세한 정보를 얻을 수 있습니다. 더 자세한 내용은 Amazon RDS용 DevOps Guru를 사용한 성능 이상 항목 분석을 참고하십시오.
- 동일한 지표의 여러 차원에 이상 항목이 있는 경우가 많습니다. 그래프로 표시된 보기에서 차원을 살펴보면 문제를 더 깊이 이해할 수 있습니다.
- 인사이트의 이벤트 섹션에서 배포 또는 인사이트가 생성될 즈음에 발생한 인프라 이벤트를 살펴보십시오. 인사이트의 비정상적인 동작이 발생했을 때 어떤 이벤트가 발생했는지 알고 있으면 문제를 이해하고 진단하는 데 도움이 될 수 있습니다.
- 운영 체제에서 인사이트와 거의 같은 시기에 발생한 티켓을 찾아 단서를 얻어 보십시오.
- 인사이트에서 권장 사항을 읽고 권장 사항에 있는 링크를 방문해 보십시오. 여기에는 문제를 신속하게 진단하고 해결하는 데 도움이 되는 문제 해결 단계가 포함되어 있는 경우가 많습니다.
- 문제를 이미 해결한 경우가 아니라면 해결된 인사이트를 그냥 무시하고 지나치지 마십시오. 문제가 해결되었더라도 하루에 한 번은 새로운 인사이트를 살펴보십시오. 가능한 한 최대한 많은 인사이트의 근본 원인을 파악하도록 노력하십시오. 시스템 문제의 징후가 될 수 있는 패턴을 찾아보십시오. 시스템 문제를 해결하지 않고 방치하면 나중에 더 심각한 문제가 발생할 수 있습니다. 일시적인 문제를 지금 해결하면 앞으로 더 심각한 사고를 예방하는 데 도움이 될 수 있습니다.

Amazon DevOpsGuru의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS Cloud에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. 는 안전하게 사용할 수 있는 서비스 AWS 도 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon DevOpsGuru에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 AWS 프로그램 범위 내 서비스 규정 준수 프로그램.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 DevOpsGuru를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 DevOpsGuru를 구성하는 방법을 보여줍니다. DevOpsGuru 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

Amazon DevOpsGuru의 데이터 보호

AWS 공동 책임 모델 Amazon DevOpsGuru의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 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 섹션을 FAQ참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 책임 공유 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management ()를 사용하여 개별 사용자를 설정하는 것이 좋습니다IAM. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 FIPS 를 AWS 통해 에 액세스할 때 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 API사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 DevOpsGuru 또는 기타 AWS 서비스 에서 콘솔, API AWS CLI또는 를 사용하여 작업하는 경우가 포함됩니다 AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL를 제공하는 경우 해당 서버에 대한 요청을 검증URL하기 위해 에 보안 인증 정보를 포함하지 않는 것이 좋습니다.

DevOpsGuru의 데이터 암호화

암호화는 DevOpsGuru 보안의 중요한 부분입니다. 전송 중인 데이터 암호화와 같은 일부 암호화 기능은 기본으로 제공되며 암호화 프로그램을 추가할 필요가 없습니다. 유휴 상태의 데이터 암호화와 같은 기타 암호화는 프로젝트나 빌드 생성 시 구성할 수 있습니다.

- 전송 중 데이터 암호화 : 고객과 DevOpsGuru 간의 모든 통신과 DevOpsGuru와 그 다운스트림 종속성 간의 모든 통신은 서명 버전 4 서명 프로세스를 사용하여 보호TLS되고 인증됩니다. 모든

DevOpsGuru 엔드포인트는 에서 관리하는 인증서를 사용합니다 AWS Private Certificate Authority. 자세한 내용은 서명 버전 4 서명 프로세스 및 정의 ACM 섹션을 참조하세요PCA.

- 저장 데이터 암호화 : DevOpsGuru에서 분석한 모든 AWS 리소스의 경우 Amazon CloudWatch 지표 및 데이터, 리소스 및 AWS CloudTrail 이벤트는 Amazon S3IDs, Amazon DynamoDB 및 Amazon Kinesis 를 사용하여 저장됩니다. AWS CloudFormation 스택을 사용하여 분석된 리소스를 정의하는 경우 스택 데이터도 수집됩니다. DevOpsGuru는 Amazon S3, DynamoDB 및 Kinesis의 데이터 보존 정책을 사용합니다. Kinesis에 저장된 데이터는 최대 1년 동안 보존될 수 있으며 정해진 정책에 따라 달라집니다. Amazon S3와 DynamoDB에 저장된 데이터는 1년 동안 저장됩니다.

  저장된 데이터는 Amazon S3, DynamoDB 및 Kinesis의 암호화 기능을 사용하여 data-at-rest 암호화됩니다.

  고객 관리형 키 : DevOpsGuru는 고객 관리형 키를 사용하여 CloudWatch Logs에서 생성된 로그 이상과 같은 민감한 메타데이터와 고객 콘텐츠 암호화를 지원합니다. 이 기능은 조직의 규정 준수 및 규제 요구 사항을 충족하는 데 도움이 되는 자체 관리형 보안 계층을 추가할 수 있는 옵션을 제공합니다. DevOpsGuru 설정에서 고객 관리형 키를 활성화하는 방법에 대한 자세한 내용은 섹션을 참조하세요the section called “암호화 업데이트”.

  이 암호화 계층을 완전히 제어할 수 있으므로 다음과 같은 작업을 수행할 수 있습니다.

  - 키 정책 수립 및 유지
  - IAM 정책 및 권한 부여 설정 및 유지
  - 키 정책 활성화 및 비활성화
  - 키 암호화 자료 교체
  - 태그 추가
  - 키 별칭 생성
  - 삭제를 위한 스케줄 키

  자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 관리형 키를 참조하세요.

  > **Note**
  >
  > DevOpsGuru는 AWS 소유 키를 사용하여 저장 시 암호화를 자동으로 활성화하여 민감한 메타데이터를 무료로 보호합니다. 그러나 고객 관리형 키를 사용하는 경우 AWS KMS 요금이 부과됩니다. 요금에 대한 자세한 내용은 AWS Key Management Service 요금을 참조하세요.

DevOpsGuru가 에서 권한 부여를 사용하는 방법 AWS KMS

DevOpsGuru는 고객 관리형 키를 사용하려면 권한 부여가 필요합니다.

고객 관리형 키를 사용하여 암호화를 활성화하도록 선택하면 DevOpsGuru는 에 CreateGrant 요청을 보내 사용자를 대신하여 권한을 생성합니다 AWS KMS. 의 권한 부여 AWS KMS 는 DevOpsGuru에게 고객 계정의 AWS KMS 키에 대한 액세스 권한을 부여하는 데 사용됩니다.

DevOpsGuru는 다음과 같은 내부 작업에 고객 관리형 키를 사용하려면 권한 부여가 필요합니다.

- 트래커 또는 지오펜스 컬렉션을 생성할 때 입력한 대칭 고객 관리형 KMS 키 ID가 유효한지 AWS KMS 확인하려면 에 DescribeKey 요청을 보냅니다.
- AWS KMS 에 GenerateDataKey 요청을 보내 고객 관리형 키로 암호화된 데이터 키를 생성합니다.
- AWS KMS 에 복호화 요청을 보내 암호화된 데이터 키를 복호화하여 데이터를 암호화하는 데 사용할 수 있도록 합니다.

언제든지 권한 부여에 대한 액세스 권한을 취소하거나 고객 관리형 키에 대한 서비스 액세스를 제거할 수 있습니다. 이렇게 하면 DevOpsGuu는 고객 관리형 키로 암호화된 데이터에 액세스할 수 없으며, 이는 해당 데이터에 의존하는 작업에 영향을 미칩니다. 예를 들어 DevOpsGuru가 액세스할 수 없는 암호화된 로그 이상 정보를 가져오려고 하면 작업이 AccessDeniedException 오류를 반환합니다.

DevOpsGuru에서 암호화 키 모니터링

DevOpsGuru 리소스와 함께 AWS KMS 고객 관리형 키를 사용하는 경우 AWS CloudTrail 또는 CloudWatch 로그를 사용하여 DevOpsGuru가 에 보내는 요청을 추적할 수 있습니다 AWS KMS.

고객 관리형 키 생성

AWS Management Console 또는 를 사용하여 대칭 고객 관리형 키를 생성할 수 있습니다 AWS KMS APIs.

대칭 고객 관리형 키를 생성하려면 대칭 암호화 KMS 키 생성을 참조하세요.

키 정책

키 정책은 고객 관리형 키에 대한 액세스를 제어합니다. 모든 고객 관리형 키에는 키를 사용할 수 있는 사람과 키를 사용하는 방법을 결정하는 문장이 포함된 정확히 하나의 키 정책이 있어야 합니다. 고객 관리형 키를 생성할 때 키 정책을 지정할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 인증 및 액세스 제어를 AWS KMS 참조하세요.

고객 관리형 키를 DevOpsGuru 리소스와 함께 사용하려면 키 정책에서 다음 API 작업을 허용해야 합니다.

- `kms:CreateGrant` - 고객 관리형 키에 권한 부여를 추가합니다. DevOpsGuru가 요구하는 작업에 대한 액세스를 허용하는 지정된 AWS KMS 키에 대한 제어 액세스 권한을 부여합니다. 권한 부여 사용에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요.

이렇게 하면 DevOpsGuru가 다음을 수행할 수 있습니다.

- 데이터 키는 즉시 암호화 GenerateDataKey 에 사용되지 않으므로 를 호출하여 암호화된 데이터 키를 생성하고 저장합니다.
- 저장된 상태의 암호화된 데이터 키를 사용하여 암호화된 데이터에 액세스하려면 Decrypt를 호출합니다.
- 서비스가 에 허용되도록 사용 중지 보안 주체를 설정합니다 RetireGrant.
- DevOpsGuru가 키를 검증할 수 있도록 고객 관리형 키 세부 정보를 kms:DescribeKey 제공하는 데 사용합니다.

다음 문에는 DevOpsGuru에 추가할 수 있는 정책 문 예제가 포함되어 있습니다.

```
"Statement" : [
  {
    "Sid" : "Allow access to principals authorized to use DevOps Guru",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "devops-guru.Region.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
  },
  {
    "Sid": "Allow access for key administrators",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
       },
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*"
      ],
      "Resource" : "*"
    }
  ]
```

트래픽 개인 정보 보호

인터페이스 VPC 엔드포인트를 사용하도록 DevOpsGuru를 구성하여 리소스 분석 및 인사이트 생성의 보안을 개선할 수 있습니다. 이렇게 하려면 인터넷 게이트웨이, NAT 디바이스 또는 가상 프라이빗 게이트웨이가 필요하지 않습니다. 또한 를 구성할 필요는 없지만 를 구성하는 PrivateLink것이 좋습니다. 자세한 내용은 DevOpsGuru 및 인터페이스 VPC 엔드포인트(AWS PrivateLink) 단원을 참조하십시오. PrivateLink 및 VPC 엔드포인트에 대한 자세한 내용은 AWS PrivateLink 및 를 통한 AWS 서비스 액세스를 참조하세요 PrivateLink.

Amazon DevOpsGuru용 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 DevOpsGuru 리소스를 사용할 수 있는 인증(로그인) 및 권한 부여(권한 보유) 대상을 제어합니다. IAM 는 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

고객

AWS Identity and Access Management (IAM) 사용 방법은 DevOpsGuru에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - DevOpsGuru 서비스를 사용하여 작업을 수행하는 경우 관리자는 필요한 자격 증명과 권한을 제공합니다. 더 많은 DevOpsGuru 기능을 사용하여 작업을 수행하려면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. DevOpsGuru에서 기능에 액세스할 수 없는 경우 섹션을 참조하세요Amazon DevOpsGuru 자격 증명 및 액세스 문제 해결.

서비스 관리자 - 회사에서 DevOpsGuru 리소스를 담당하는 경우 DevOpsGuru에 대한 전체 액세스 권한이 있을 수 있습니다. 서비스 사용자가 액세스해야 하는 DevOpsGuru 기능과 리소스를 결정하는 것은 사용자의 작업입니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 이해합니다IAM. 회사에서 DevOpsGuruIAM를 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요Amazon DevOpsGuru의 작동 방식 IAM.

IAM 관리자 - IAM 관리자인 경우 DevOpsGuru에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. 에서 사용할 수 있는 DevOpsGuru 자격 증명 기반 정책 예제를 보려면 섹션을 IAM참조하세요Amazon DevOpsGuru에 대한 자격 증명 기반 정책.

ID를 통한 인증

인증은 자격 증명 AWS 으로 에 로그인하는 방법입니다. 로 AWS 계정 루트 사용자, IAM 사용자로 또는 IAM 역할을 수임하여 인증(에 로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 에 페더레이션 자격 증명 AWS 으로 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션 자격 증명으로 로그인하면 관리자가 이전에 IAM 역할을 사용하여 자격 증명 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 에 로그인하는 방법을 AWS 계정 AWS참조하세요.

AWS 프로그래밍 방식으로 에 액세스하는 경우 는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공하여 자격 증명을 사용하여 요청에 암호화 방식으로 서명합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 요청 서명을 AWS API 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 사용 설명서의 다중 인증 사용(MFA) AWS을 참조하세요IAM.

AWS 계정 루트 사용자

를 생성하면 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, , AWS Directory Service Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비

스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명이 에 액세스하면 역할을 AWS 계정수임하고 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 및 애플리케이션에서 사용할 수 있도록 자체 자격 증명 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능한 경우 암호 및 액세스 키와 같은 장기 보안 인증 정보가 있는 IAM 사용자를 생성하는 대신 임시 보안 인증 정보를 사용하는 것이 좋습니다. 그러나 IAM 사용자와 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례에 대한 액세스 키 정기적으로 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 라는 그룹을 지정IAMAdmins하고 해당 그룹에 IAM 리소스를 관리할 수 있는 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 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 (역할 대신) IAM 사용자를 생성할 시기를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 비슷하지만 특정 사람과는 연결되지 않습니다. IAM 역할을 전환 AWS Management Console 하여 에서 역할을 일시적으로 수임할 수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출 AWS CLI 하거나 사용자 지정 를 사용하여 역할을 수임할 수 있습니다URL. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자에 대한 역할 생성을

참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 의 역할과 상호 연관시킵니다IAM. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 특정 작업에 대해 일시적으로 다른 권한을 맡을 IAM 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 누군가(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 에서 교차 계정 리소스 액세스를 IAM 참조하세요.
- 교차 서비스 액세스 - 일부 는 다른 에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가 Amazon에서 애플리케이션을 실행EC2하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하면 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 액세스 세션 전달을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 에 권한을 위임할 역할 생성을 AWS 서비스 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon에서 실행되는 애플리케이션 EC2 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 보안 인증을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장하는 것보다 좋습니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행 중인 프로그램이 임시 보안 인증을 가져올 수 있습니다. 자세한 내용은 IAM 사용 설명서EC2의 IAM 역할 사용을 참조하세요.

IAM 역할 또는 IAM 사용자를 사용할지 여부를 알아보려면 IAM 사용 설명서의 IAM 역할 생성 시기(사용자 대신)를 참조하세요.

정책을 사용한 액세스 관리

정책을 AWS 생성하고 AWS 자격 증명 또는 리소스에 연결하여 의 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는 의 객체입니다. 는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 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 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI또는 에서 역할 정보를 가져올 수 있습니다 AWS API.

보안 인증 기반 정책

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 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소

스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 가 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책IAM에서는 의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs 는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지는 않습니다.

Amazon S3 AWS WAF및 AmazonVPC은 를 지원하는 서비스의 예입니다ACLs. 에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 ACLs참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 자격 증명 기반 정책이 IAM엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - 의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책 SCPs입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러 을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직의 모든 기능을 활성화하면 서비스 제어 정책(SCPs)을 모든 또는 일부 계정에 적용할 수 있습니다. 는 각 를 포함하여 멤버 계정의 엔터티에 대한 권한을 SCP 제한합니다 AWS 계정 루트 사용자. 조직 및 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 SCPs참조하세요.
- 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 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. AWS 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

DevOps AWS 관리형 정책 및 서비스 연결 역할에 대한 Guru 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 DevOpsGuru의 AWS 관리형 정책 및 서비스 연결 역할에 대한 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 DevOpsGuru의 RSS 피드를 구독하세요Amazon DevOps Guru 문서 기록.

변경 사항	설명	날짜
AmazonDevOpsGuruConsoleFullAccess - 기존 정책에 대한 업데이트	`AmazonDevOpsGuruFullAccess` 관리형 정책은 이제 Amazon SNS 구독을 지원합니다.	2023년 8월 9일
AmazonDevOpsGuruReadOnlyAccess -기존 정책 업데이트	이제 `AmazonDevOpsGuruReadOnlyAccess` 관리형 정책은 Amazon SNS 구독 목록에 대한 읽기 전용 액세스를 지원합니다.	2023년 8월 9일
AmazonDevOpsGuruServiceRolePolicy - 기존 정책에 대한 업데이트	이제 `AWSServiceRoleForDevOpsGuru` 서비스 연결 역할이 REST 에서 API 게이트웨이 GET 작업에 대한 액세스를 지원합니다APIs.	2023년 1월 11일
AmazonDevOpsGuruServiceRolePolicy - 기존 정책에 대한 업데이트	이제 `AWSServiceRoleForDevOpsGuru` 서비스 연결 역할에서는 여러 가지 Amazon Simple Storage Service 및 Service Quotas 작업을 지원합니다.	2022년 10월 19일

변경 사항	설명	날짜
AmazonDevOpsGuruFullAccess -기존 정책 업데이트	`AmazonDevOpsGuruFullAccess` 관리형 정책 는 CloudWatch `FilterLogEvents` 이제 작업에 대한 액세스를 지원합니다.	2022년 8월 30일
AmazonDevOpsGuruConsoleFullAccess -기존 정책 업데이트	이제 `AmazonDevOpsGuruConsoleFullAccess` 관리형 정책이 `FilterLogEvents` 작업에 대한 CloudWatch 액세스를 지원합니다.	2022년 8월 30일
AmazonDevOpsGuruReadOnlyAccess -기존 정책 업데이트	`AmazonDevOpsGuruReadOnlyAccess` 관리형 정책은 이제 작업에 대한 CloudWatch `FilterLogEvents` 읽기 전용 액세스를 지원합니다.	2022년 8월 30일
AmazonDevOpsGuruServiceRolePolicy - 기존 정책에 대한 업데이트	`AWSServiceRoleForDevOpsGuru` 서비스 연결 역할은 이제 CloudWatch 로그 작업 `FilterLogEvents` , `DescribeLogGroups` 및 를 지원합니다`DescribeLogStreams` .	2022년 7월 12일
DevOpsGuru에 대한 자격 증명 기반 정책 - 새로운 관리형 정책.	`AmazonDevOpsGuruConsoleFullAccess` 정책이 추가되었습니다.	2021년 12월 16일

변경 사항	설명	날짜
AmazonDevOpsGuruServiceRolePolicy - 기존 정책에 대한 업데이트	`AWSServiceRoleForDevOpsGuru` 서비스 연결 역할은 이제 성능 개선 도우미 `DescribeMetricsKeys` 및 Amazon RDS `DescribeDBInstances` 작업을 지원합니다.	2021년 12월 1일
AmazonDevOpsGuruReadOnlyAccess -기존 정책 업데이트	이제 `AmazonDevOpsGuruReadOnlyAccess` 관리형 정책은 Amazon RDS `DescribeDBInstances` 작업에 대한 읽기 전용 액세스를 지원합니다.	2021년 12월 1일
AmazonDevOpsGuruFullAccess -기존 정책 업데이트	`AmazonDevOpsGuruFullAccess` 관리형 정책은 이제 Amazon RDS `DescribeDBInstances` 작업에 대한 액세스를 지원합니다.	2021년 12월 1일
Amazon DevOpsGuru에 대한 자격 증명 기반 정책 – 새 정책을 추가했습니다.	이제 `AWSServiceRoleForDevOpsGuru` 서비스 연결 역할이 Amazon RDS `DescribeDBInstances` 및 성능 개선 도우미 `GetResourceMetrics` 작업에 대한 액세스를 지원합니다. `AmazonDevOpsGuruOrganizationsAccess` 관리형 정책은 조직 내에서 DevOpsGuru에 대한 액세스를 제공합니다.	2021년 11월 16일

변경 사항	설명	날짜
AmazonDevOpsGuruServiceRolePolicy - 기존 정책에 대한 업데이트	이제 `AWSServiceRoleForDevOpsGuru` 서비스 연결 역할이 AWS Organizations를 지원합니다.	2021년 11월 4일
AmazonDevOpsGuruServiceRolePolicy - 기존 정책에 대한 업데이트	이제 `AWSServiceRoleForDevOpsGuru` 서비스 연결 역할에 `ssm:CreateOpsItem` 및 `ssm:AddTagsToResource` 작업에 대한 새로운 조건이 포함됩니다.	2021년 10월 11일
DevOpsGuru에 대한 서비스 연결 역할 권한 - 기존 정책에 대한 업데이트	이제 `AWSServiceRoleForDevOpsGuru` 서비스 연결 역할에 `ssm:CreateOpsItem` 및 `ssm:AddTagsToResource` 작업에 대한 새로운 조건이 포함됩니다.	2021년 6월 14일
AmazonDevOpsGuruReadOnlyAccess -기존 정책 업데이트	이제 `AmazonDevOpsGuruReadOnlyAccess` 관리형 정책에서 및 DevOpsGuru `DescribeFeedback` 작업에 대한 AWS Identity and Access Management `GetRole` 읽기 전용 액세스를 허용합니다.	2021년 6월 14일
AmazonDevOpsGuruReadOnlyAccess -기존 정책 업데이트	`AmazonDevOpsGuruReadOnlyAccess` 관리형 정책은 이제 DevOpsGuru `GetCostEstimation` 및 `StartCostEstimation` 작업에 대한 읽기 전용 액세스를 허용합니다.	2021년 4월 27일

변경 사항	설명	날짜
AmazonDevOpsGuruServiceRolePolicy - 기존 정책에 대한 업데이트	이제 `AWSServiceRoleForDevOpsGuru` 역할은 및 Amazon EC2 Auto Scaling `DescribeAutoScalingGroups` 작업에 대한 AWS Systems Manager `AddTagsToResource` 액세스를 허용합니다.	2021년 4월 27일
DevOpsGuru가 변경 사항 추적 시작	DevOpsGuru는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2020년 12월 10일

Amazon DevOpsGuru의 작동 방식 IAM

IAM 를 사용하여 DevOpsGuru에 대한 액세스를 관리하기 전에 DevOpsGuru에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

IAM Amazon DevOpsGuru와 함께 사용할 수 있는 기능

IAM 기능	DevOpsGuru 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC (정책의 태그)	아니요

IAM 기능	DevOpsGuru 지원
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 링크 역할	예

DevOpsGuru 및 기타 AWS 서비스가 대부분의 IAM 기능에서 작동하는 방식을 개괄적으로 알아보려면 IAM 사용 설명서의 에서 AWS 를 사용하는 서비스를 IAM 참조하세요.

DevOpsGuru에 대한 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 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부된 작업 및 리소스와 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

DevOpsGuru의 자격 증명 기반 정책 예제

DevOpsGuru 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon DevOpsGuru에 대한 자격 증명 기반 정책.

DevOpsGuru 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 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 있는지를

정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려면 리소스 기반 정책의 보안 주체로 전체 계정 또는 다른 계정의 IAM엔터티를 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 에 있는 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 개체(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 에서 크로스 계정 리소스 액세스를 IAM 참조하세요.

DevOpsGuru에 대한 정책 작업

정책 작업 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 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 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 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.

DevOpsGuru 작업 목록을 보려면 서비스 승인 참조의 Amazon DevOpsGuru에서 정의한 작업을 참조하세요.

DevOpsGuru의 정책 작업은 작업 전에 다음 접두사를 사용합니다.

```
aws
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "aws:action1",
      "aws:action2"
         ]
```

DevOpsGuru 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon DevOpsGuru에 대한 자격 증명 기반 정책.

DevOpsGuru에 대한 정책 리소스

정책 리소스 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 객체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 가장 좋은 방법은 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정하는 것입니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

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

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

DevOpsGuru 리소스 유형 및 해당 의 목록을 보려면 서비스 권한 부여 참조의 Amazon DevOpsGuru에서 정의한 리소스를 ARNs참조하세요. 각 리소스ARN의 를 지정할 수 있는 작업을 알아보려면 Amazon DevOpsGuru에서 정의한 작업을 참조하세요.

DevOpsGuru 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon DevOpsGuru에 대한 자격 증명 기반 정책.

DevOpsGuru의 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 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 논리

적 OR 작업을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

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

AWS 는 전역 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

DevOpsGuru 조건 키 목록을 보려면 서비스 권한 부여 참조의 Amazon DevOpsGuru에 대한 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 Amazon DevOpsGuru에서 정의한 작업을 참조하세요.

DevOpsGuru 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Amazon DevOpsGuru에 대한 자격 증명 기반 정책.

DevOpsGuru의 액세스 제어 목록(ACLs)

지원 ACLs: 아니요

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs 는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지는 않습니다.

DevOpsGuru를 사용한 속성 기반 액세스 제어(ABAC)

지원ABAC(정책의 태그): 아니요

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그 라고 합니다. IAM 엔터티(사용자 또는 역할) 및 여러 AWS 리소스에 태그를 연결할 수 있습니다. 엔터티 및 리소스에 태그를 지정하는 것은 의 첫 번째 단계입니다ABAC. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계합니다.

ABAC 는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로워지는 상황에 도움이 됩니다.

태그에 근거하여 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 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

에 대한 자세한 내용은 IAM 사용 설명서의 란 무엇입니까ABAC?를 ABAC참조하세요. 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어 사용(ABAC)을 ABAC참조하세요.

DevOpsGuru에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인할 때 작동하지 AWS 서비스 않는 경우도 있습니다. 임시 자격 증명으로 AWS 서비스 작업하는 경우를 비롯한 자세한 내용은 IAM 사용 설명서의 AWS 서비스 에서 작업하는 IAM 섹션을 참조하세요.

사용자 이름 및 암호를 제외한 방법을 AWS Management Console 사용하여 에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 Single Sign-On(SSO) 링크를 AWS 사용하여 에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할(콘솔) 전환을 참조하세요.

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS API. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 AWS. AWS recommends에 액세스할 수 있습니다. 자세한 내용은 의 임시 보안 자격 증명을 IAM참조하세요.

DevOpsGuru에 대한 교차 서비스 보안 주체 권한

전달 액세스 세션 지원(FAS): 예

IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하면 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 액세스 세션 전달을 참조하세요.

DevOpsGuru의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 에 권한을 위임할 역할 생성을 AWS 서비스 참조하세요.

> **Warning**
> 서비스 역할에 대한 권한을 변경하면 DevOpsGuru 기능이 중단될 수 있습니다. DevOpsGuru 가 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

DevOpsGuru의 서비스 연결 역할

서비스 링크 역할 지원: 예

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 AWS 에서 작동하는 서비스를 참조하세요IAM. 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

Amazon DevOpsGuru에 대한 자격 증명 기반 정책

기본적으로 사용자 및 역할에는 DevOpsGuru 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 를 사용하여 작업을 수행할 수 없습니다 AWS API. 사용자에게 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하기 위해 IAM 관리자는 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수임할 수 있습니다.

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

각 리소스 유형에 ARNs 대한 형식 등 DevOpsGuru에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 Amazon DevOpsGuru에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- DevOpsGuru 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- AWS DevOpsGuru에 대한 관리형(미리 정의된) 정책

정책 모범 사례

자격 증명 기반 정책은 계정에서 DevOpsGuru 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 관리AWS 형 정책 또는 AWS 작업 함수에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 - IAM 정책으로 권한을 설정할 때 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 적용하는 IAM 방법에 대한 자세한 내용은 IAM 사용 설명서의 에서 정책 및 권한을 IAM 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 정책 조건을 작성하여 를 사용하여 모든 요청을 전송하도록 지정할 수 있습니다SSL. AWS 서비스와 같은 특정 를 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 정책이 정책 언어(JSON) 및 IAM 모범 사례를 준수하도록 새 정책 및 기존 IAM 정책을 검증합니다. IAM Access Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 확인 및 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 다중 인증 필요(MFA) - 에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 MFA 위해 를 AWS 계정켭니다. API 작업을 호출할 MFA 때 를 요구하려면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA-보호된 API 액세스 구성을 참조하세요.

의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 의 보안 모범 사례를 IAM IAM참조하세요.

DevOpsGuru 콘솔 사용

Amazon DevOpsGuru 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 에서 DevOpsGuru 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다 AWS 계정. 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 에만 전화를 거는 사용자에 대해 최소 콘솔 권한을 허용할 필요는 없습니다 AWS API. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 허용합니다.

사용자와 역할이 DevOpsGuru 콘솔을 계속 사용할 수 있도록 하려면 DevOpsGuru `AmazonDevOpsGuruReadOnlyAccess` 또는 `AmazonDevOpsGuruFullAccess` AWS 관리형 정책을 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함되어 있습니다 AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS DevOpsGuru에 대한 관리형(미리 정의된) 정책

AWS 는 에서 생성 및 관리하는 독립 실행형 IAM 정책을 제공하여 많은 일반적인 사용 사례를 처리합니다 AWS. 이러한 AWS관리형 정책은 일반적인 사용 사례에 필요한 권한을 부여하므로 필요한 권한을 조사할 필요가 없습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

DevOpsGuru 서비스 역할을 생성하고 관리하려면 라는 AWS관리형 정책도 연결해야 합니다`IAMFullAccess`.

DevOpsGuru 작업 및 리소스에 대한 권한을 허용하는 사용자 지정 IAM 정책을 생성할 수도 있습니다. 해당 권한이 필요한 사용자 또는 그룹에 이러한 사용자 지정 정책을 연결할 수 있습니다.

계정의 사용자에게 연결할 수 있는 다음과 같은 AWS관리형 정책은 DevOpsGuru에만 적용됩니다.

주제

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess` - Amazon SNS 주제 생성, Amazon CloudWatch 지표 액세스 및 AWS CloudFormation 스택 액세스 권한을 포함하여 DevOpsGuru에 대한 전체 액세스를 제공합니다. DevOpsGuru에 대한 전체 제어 권한을 부여하려는 관리 수준 사용자에게만 이 옵션을 적용합니다.

`AmazonDevOpsGuruFullAccess` 정책에는 다음과 같은 문장이 포함되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess` - Amazon SNS 주제 CloudWatch 생성, Amazon 지표 액세스 및 AWS CloudFormation 스택 액세스 권한을 포함하여 DevOpsGuru에 대한 전체 액세스를 제공합니다. 이 정책에는 콘솔에서 이상 Amazon RDS Aurora DB 인스턴스와 관련된 자세한 분석을 볼 수 있도록 추가 성능 인사이트 권한이 있습니다. DevOpsGuru에 대한 전체 제어 권한을 부여하려는 관리 수준 사용자에게만 이 내용을 적용합니다.

`AmazonDevOpsGuruConsoleFullAccess` 정책에는 다음과 같은 문장이 포함되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
```

```
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "PerformanceInsightsMetricsDataAccess",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruReadOnlyAccess

`AmazonDevOpsGuruReadOnlyAccess` – DevOpsGuru 및 다른 AWS 서비스의 관련 리소스에 대한 읽기 전용 액세스 권한을 부여합니다. 이 정책을 인사이트를 볼 수 있는 기능을 부여하려는 사용자에게 적용하되 DevOpsGuru의 분석 범위 경계, Amazon SNS 주제 또는 Systems Manager OpsCenter 통합을 업데이트하지는 않습니다.

`AmazonDevOpsGuruReadOnlyAccess` 정책에는 다음과 같은 문장이 포함되어 있습니다.

```
    {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruReadOnlyAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "devops-guru:DescribeAccountHealth",
                "devops-guru:DescribeAccountOverview",
                "devops-guru:DescribeAnomaly",
                "devops-guru:DescribeEventSourcesConfig",
                "devops-guru:DescribeFeedback",
                "devops-guru:DescribeInsight",
                "devops-guru:DescribeResourceCollectionHealth",
                "devops-guru:DescribeServiceIntegration",
                "devops-guru:GetCostEstimation",
                "devops-guru:GetResourceCollection",
                "devops-guru:ListAnomaliesForInsight",
                "devops-guru:ListEvents",
                "devops-guru:ListInsights",
                "devops-guru:ListAnomalousLogGroups",
                "devops-guru:ListMonitoredResources",
                "devops-guru:ListNotificationChannels",
                "devops-guru:ListRecommendations",
                "devops-guru:SearchInsights",
                "devops-guru:StartCostEstimation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruOrganizationsAccess

`AmazonDevOpsGuruOrganizationsAccess` - Organizations 관리자에게 조직 내 DevOpsGuru 다중 계정 보기에 대한 액세스 권한을 제공합니다. 조직 내에서 DevOpsGuru에 대한 전체 액세스 권한을 부여하려는 조직의 관리자 수준 사용자에게 이 정책을 적용합니다. 조직의 관리 계정과 DevOpsGuru의 위임된 관리자 계정에 이 정책을 적용할 수 있습니다. 이 정책에 추가하여

AmazonDevOpsGuruReadOnlyAccess 또는 AmazonDevOpsGuruFullAccess 를 적용하여 DevOpsGuru에 대한 읽기 전용 또는 전체 액세스를 제공할 수 있습니다.

AmazonDevOpsGuruOrganizationsAccess 정책에는 다음과 같은 문장이 포함되어 있습니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDevOpsGuruOrganizationsAccess",
   "Effect": "Allow",
   "Action": [
    "devops-guru:DescribeOrganizationHealth",
    "devops-guru:DescribeOrganizationResourceCollectionHealth",
    "devops-guru:DescribeOrganizationOverview",
    "devops-guru:ListOrganizationInsights",
    "devops-guru:SearchOrganizationInsights"
   ],
   "Resource": "*"
  },
  {
   "Sid": "OrganizationsDataAccess",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccounts",
    "organizations:ListChildren",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListRoots"
   ],
   "Resource": "arn:aws:organizations::*:"
  },
  {
   "Sid": "OrganizationsAdminDataAccess",
   "Effect": "Allow",
   "Action": [
    "organizations:DeregisterDelegatedAdministrator",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
```

```
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "devops-guru.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

DevOpsGuru에 대한 서비스 연결 역할 사용

Amazon DevOpsGuru는 AWS Identity and Access Management (IAM) 서비스 연결 역할 을 사용합니다. 서비스 연결 역할은 DevOpsGuru에 직접 연결되는 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 DevOpsGuru에서 사전 정의하며 서비스에서 사용자를 대신하여 AWS CloudTrail, Amazon CloudWatch, AWS CodeDeploy, AWS X-Ray및 AWS Organizations를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 DevOpsGuru를 더 쉽게 설정할 수 있습니다. DevOpsGuru는 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 DevOpsGuru만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책 및 권한 정책이 포함되며 해당 권한 정책은 다른 IAM엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 수 없으므로 DevOpsGuru 리소스를 보호합니다.

DevOpsGuru에 대한 서비스 연결 역할 권한

DevOpsGuru는 라는 서비스 연결 역할을 사용합니다`AWSServiceRoleForDevOpsGuru`. 이 정책은 DevOpsGuru가 계정에서 실행해야 하는 범위가 지정된 권한이 있는 AWS 관리형 정책입니다.

`AWSServiceRoleForDevOpsGuru` 서비스 연결 역할은 그 역할을 위임하기 위해 다음 서비스를 신뢰합니다.

- `devops-guru.amazonaws.com`

역할 권한 정책은 DevOpsGuru가 지정된 리소스에 대해 다음 작업을 완료할 수 있도록 `AmazonDevOpsGuruServiceRolePolicy` 허용합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "cloudtrail:LookupEvents",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "cloudwatch:DescribeAnomalyDetectors",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:ListDashboards",
    "cloudwatch:GetDashboard",
    "cloudformation:GetTemplate",
    "cloudformation:ListStacks",
    "cloudformation:ListStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:ListImports",
    "codedeploy:BatchGetDeployments",
    "codedeploy:GetDeploymentGroup",
    "codedeploy:ListDeployments",
    "config:DescribeConfigurationRecorderStatus",
    "config:GetResourceConfigHistory",
    "events:ListRuleNamesByTarget",
    "xray:GetServiceGraph",
    "organizations:ListRoots",
    "organizations:ListChildren",
    "organizations:ListDelegatedAdministrators",
    "pi:GetResourceMetrics",
    "tag:GetResources",
    "lambda:GetFunction",
    "lambda:GetFunctionConcurrency",
    "lambda:GetAccountSettings",
    "lambda:ListProvisionedConcurrencyConfigs",
    "lambda:ListAliases",
    "lambda:ListEventSourceMappings",
    "lambda:GetPolicy",
    "ec2:DescribeSubnets",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingPolicies",
    "sqs:GetQueueAttributes",
    "kinesis:DescribeStream",
```

```
    "kinesis:DescribeLimits",
    "dynamodb:DescribeTable",
    "dynamodb:DescribeLimits",
    "dynamodb:DescribeContinuousBackups",
    "dynamodb:DescribeStream",
    "dynamodb:ListStreams",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "rds:DescribeOptionGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeAccountAttributes",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "s3:GetBucketNotification",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketWebsite",
    "s3:GetIntelligentTieringConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowPutTargetsOnASpecificRule",
   "Effect": "Allow",
   "Action": [
    "events:PutTargets",
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
  },
  {
   "Sid": "AllowCreateOpsItem",
   "Effect": "Allow",
```

```
    "Action": [
     "ssm:CreateOpsItem"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowAddTagsToOpsItem",
    "Effect": "Allow",
    "Action": [
     "ssm:AddTagsToResource"
    ],
    "Resource": "arn:aws:ssm:*:*:opsitem/*"
   },
   {
    "Sid": "AllowAccessOpsItem",
    "Effect": "Allow",
    "Action": [
     "ssm:GetOpsItem",
     "ssm:UpdateOpsItem"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated": "true"
     }
    }
   },
   {
    "Sid": "AllowCreateManagedRule",
    "Effect": "Allow",
    "Action": "events:PutRule",
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowAccessManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowOtherOperationsOnManagedRule",
```

```
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "devops-guru.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowTagBasedFilterLogEvents",
    "Effect": "Allow",
    "Action": [
     "logs:FilterLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-Guru-Analysis": "true"
     }
    }
   },
   {
    "Sid": "AllowAPIGatewayGetIntegrations",
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": [
     "arn:aws:apigateway:*::/restapis/??????????",
     "arn:aws:apigateway:*::/restapis/*/resources",
     "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
    ]
   }
  ]
}
```

DevOpsGuru에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI또는 에서 인사이트를 생성하면 AWS API DevOpsGuru가 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이 서비스 연결 역할은 이 역할에서 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료한 경우 계정에 표시될 수 있습니다. 예를 들어 의 리포지토리에 DevOpsGuru를 추가한 경우 나타날 수 있습니다 AWS CodeCommit.

DevOpsGuru의 서비스 연결 역할 편집

DevOpsGuru에서는 `AWSServiceRoleForDevOpsGuru` 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 를 사용하여 역할에 대한 설명을 편집할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

DevOpsGuru에 대한 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, 먼저 모든 리포지토리와의 연결을 끊어야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 DevOpsGuru 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

를 사용하여 서비스 연결 역할을 수동으로 삭제하려면 IAM

IAM 콘솔, AWS CLI또는 AWS API 를 사용하여 `AWSServiceRoleForDevOpsGuru` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

Amazon DevOpsGuru 권한 참조

DevOpsGuru 정책에서 AWS전체 조건 키를 사용하여 조건을 표현할 수 있습니다. 목록은 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

정책의 `Action` 필드에 작업을 지정합니다. 작업을 지정하려면 `devops-guru:` 접두사 뒤에 API 작업 이름(예: `devops-guru:SearchInsights` 및)을 사용합니다`devops-guru:ListAnomalies`. 문장 하나에 여러 작업을 지정하려면 쉼표로 구분합니다(예: `"Action": [ "devops-guru:SearchInsights", "devops-guru:ListAnomalies" ]`).

와일드카드 문자 사용

와일드카드 문자(*ARN)가 있거나 없는 Amazon 리소스 이름()을 정책 `Resource` 필드의 리소스 값으로 지정합니다. 와일드카드를 사용하여 여러 작업 또는 리소스를 지정할 수 있습니다. 예를 들어 `devops-guru:*`는 모든 DevOpsGuru 작업을 지정하고 는 단어로 시작하는 모든 DevOpsGuru 작업을 `devops-guru:List*` 지정합니다`List`. 다음 예제에서는 로 시작하는 범용 고유 식별자(UUID)가 있는 모든 인사이트를 참조합니다`12345`.

```
arn:aws:devops-guru:us-east-2:123456789012:insight:12345*
```

IAM 자격 증명에 연결할 수 있는 권한 정책(자격 증명 기반 정책)을 설정하고 ID를 통한 인증 작성할 때 다음 테이블을 참조로 사용할 수 있습니다.

DevOpsGuru API 작업 및 작업에 필요한 권한

`AddNotificationChannel`

작업: `devops-guru:AddNotificationChannel`

DevOpsGuru의 알림 채널을 추가하는 데 필요합니다. 알림 채널은 DevOpsGuru가 작업을 개선하는 방법에 대한 정보가 포함된 인사이트를 생성할 때 이를 알리는 데 사용됩니다.

리소스: *

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

DevOpsGuru에서 알림 채널을 제거하는 데 필요합니다. 알림 채널은 DevOpsGuru가 작업을 개선하는 방법에 대한 정보가 포함된 인사이트를 생성할 때 이를 알리는 데 사용됩니다.

리소스: *

`ListNotificationChannels`

작업: `devops-guru:ListNotificationChannels`

DevOpsGuru에 대해 구성된 알림 채널 목록을 반환하는 데 필요합니다. 각 알림 채널은 DevOpsGuru가 작업을 개선하는 방법에 대한 정보가 포함된 인사이트를 생성할 때 이를 알리는 데 사용됩니다. 지원되는 알림 유형 중 하나는 Amazon Simple Notification Service (Amazon SNS)입니다.

리소스: `*`

`UpdateResourceCollectionFilter`

작업: `devops-guru:UpdateResourceCollectionFilter`

DevOpsGuru에서 계정의 어떤 AWS 리소스를 분석하는지 지정하는 데 사용되는 AWS CloudFormation 스택 목록을 업데이트하는 데 필요합니다. 분석을 통해 운영 성과를 개선하는 데 사용할 수 있는 권장 사항, 운영 지표, 운영 이벤트가 포함된 인사이트를 얻을 수 있습니다. 또한 이 메서드는 를 사용하는 데 필요한 IAM 역할을 생성합니다 CodeGuru OpsAdvisor.

리소스: `*`

`GetResourceCollectionFilter`

작업: `devops-guru:GetResourceCollectionFilter`

DevOpsGuru에서 분석하는 계정의 리소스를 지정하는 AWS 데 사용되는 AWS CloudFormation 스택 목록을 반환하는 데 필요합니다. 분석을 통해 운영 성과를 개선하는 데 사용할 수 있는 권장 사항, 운영 지표, 운영 이벤트가 포함된 인사이트를 얻을 수 있습니다.

리소스: `*`

`ListInsights`

작업: `devops-guru:ListInsights`

AWS 계정의 인사이트 목록을 반환하는 데 필요합니다. 시작 시간, 상태(`ongoing`또는`any`), 유형(`reactive`또는`predictive`) 기준으로 반환되는 인사이트를 지정할 수 있습니다.

리소스: `*`

`DescribeInsight`

작업: `devops-guru:DescribeInsight`

해당 ID를 사용하여 지정한 인사이트에 대한 세부 정보를 반환하는 데 필요합니다.

리소스: *

`SearchInsights`

작업: `devops-guru:SearchInsights`

AWS 계정의 인사이트 목록을 반환하는 데 필요합니다. 시작 시간, 필터, 유형(`reactive`또는`predictive`) 기준으로 반환되는 인사이트를 지정할 수 있습니다.

리소스: *

`ListAnomalies`

작업: `devops-guru:ListAnomalies`

해당 ID를 사용하여 지정한 인사이트에 속하는 이상 항목 목록을 반환하는 데 필요합니다.

리소스: *

`DescribeAnomaly`

작업: `devops-guru:DescribeAnomaly`

해당 ID를 사용하여 지정한 이상 항목에 대한 세부 정보를 반환하는 데 필요합니다.

리소스: *

`ListEvents`

작업: `devops-guru:ListEvents`

DevOpsGuru에서 평가한 리소스에서 내보낸 이벤트 목록을 반환하는 데 필요합니다. 필터를 사용하여 반환되는 이벤트를 지정할 수 있습니다.

리소스: *

`ListRecommendations`

작업: `devops-guru:ListRecommendations`

지정된 인사이트의 권장 사항 목록을 반환하는 데 필요합니다. 각 권장 사항에는 권장 사항과 관련된 지표 목록 및 이벤트 목록이 포함됩니다.

리소스: *

`DescribeAccountHealth`

작업: `devops-guru:DescribeAccountHealth`

미해결 대응 인사이트 수, 미해결 예측 인사이트 수, AWS 계정에서 분석된 지표 수를 반환하는 데 필요합니다. 이 숫자를 사용하여 AWS 계정의 작업 상태를 측정합니다.

리소스: *

`DescribeAccountOverview`

작업: `devops-guru:DescribeAccountOverview`

시간 범위 동안 발생한 다음을 반환하는 데 필요합니다. 생성된 미해결 대응형 인사이트 수, 생성된 미해결 예측형 인사이트 수, 종료된 모든 대응형 인사이트에 대한 평균 복구 시간(MTTR)입니다.

리소스: *

`DescribeResourceCollectionHealthOverview`

작업: `devops-guru:DescribeResourceCollectionHealthOverview`

DevOpsGuru에 지정된 각 AWS CloudFormation 스택의 모든 인사이트에 대해 열린 예측 인사이트 수, 열린 대응 인사이트 및 평균 복구 시간(MTTR)을 반환하는 데 필요합니다.

리소스: *

`DescribeIntegratedService`

작업: `devops-guru:DescribeIntegratedService`

DevOpsGuru와 통합할 수 있는 서비스의 통합 상태를 반환하는 데 필요합니다. DevOpsGuru와 통합할 수 있는 하나의 서비스는 이며 AWS Systems Manager, 생성된 각 인사이트에 OpsItem 대해를 생성하는 데 사용할 수 있습니다.

리소스: *

`UpdateIntegratedServiceConfig`

작업: `devops-guru:UpdateIntegratedServiceConfig`

DevOpsGuru와 통합할 수 있는 서비스와의 통합을 활성화하거나 비활성화하는 데 필요합니다. DevOpsGuru와 통합할 수 있는 하나의 서비스는 Systems Manager로, 생성된 각 인사이트에 OpsItem 대한 를 생성하는 데 사용할 수 있습니다.

리소스: *

Amazon SNS 주제에 대한 권한

다른 AWS 계정이 소유한 Amazon 주제에 알림을 전달하도록 Amazon DevOpsGuru를 구성하려는 경우에만 이 SNS 주제의 정보를 사용합니다.

DevOpsGuru가 다른 계정이 소유한 Amazon SNS 주제에 알림을 전송하려면 DevOpsGuru에 알림을 보낼 수 있는 권한을 부여하는 정책을 Amazon SNS 주제에 연결해야 합니다. DevOpsGuru에 사용하는 것과 동일한 계정이 소유한 Amazon SNS 주제에 알림을 전달하도록 DevOpsGuru를 구성하면 DevOpsGuru는 해당 주제에 정책을 추가합니다.

정책을 연결하여 다른 계정의 Amazon SNS 주제에 대한 권한을 구성한 후 DevOpsGuru에서 Amazon SNS 주제를 추가할 수 있습니다. 알림 채널로 Amazon SNS 정책을 업데이트하여 보안을 강화할 수도 있습니다.

> **Note**
>
> DevOpsGuru는 현재 동일한 리전에서 교차 계정 액세스만 지원합니다.

주제

다른 계정의 Amazon SNS 주제에 대한 권한 구성

IAM 역할로 권한 추가

IAM 역할로 로그인한 후 다른 계정의 Amazon SNS 주제를 사용하려면 사용하려는 Amazon SNS 주제에 정책을 연결해야 합니다. IAM 역할을 사용하는 동안 다른 계정의 Amazon SNS 주제에 정책을 연결하려면 IAM 역할의 일부로 해당 계정 리소스에 대해 다음 권한이 있어야 합니다.

- sns:CreateTopic
- sns:GetTopicAttributes

- sns:SetTopicAttributes
- sns:Publish

사용하려는 Amazon SNS 주제에 다음 정책을 연결합니다. `Resource` 키의 경우 *`topic-owner-account-id`* 는 주제 소유자의 계정 ID이며,*`topic-sender-account-id`* 는 DevOpsGuru를 설정하는 사용자의 계정 ID이며,*`devops-guru-role`* 는 관련된 개별 사용자의 IAM 역할입니다. 에 대한 적절한 값을 대체해야 합니다.*`region-id`* (예: `us-west-2`) 및 *`my-topic-name`*.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:role/devops-guru-role"]
            }
        }
    ]
}
```

IAM 사용자 권한 추가

다른 계정의 Amazon SNS 주제를 IAM 사용자로 사용하려면 다음 정책을 사용하려는 Amazon SNS 주제에 연결합니다. `Resource` 키의 경우 *`topic-owner-account-id`* 는 주제 소유자의 계정 ID

이며,*topic-sender-account-id* 는 DevOpsGuru를 설정하는 사용자의 계정 ID이며,*devops-guru-user-name* 는 관련된 개별 IAM 사용자입니다. 에 대한 적절한 값을 대체해야 합니다.*region-id* (예: `us-west-2`) 및 *my-topic-name*.

> **Note**
>
> 가능한 경우 암호 및 액세스 키와 같은 장기 보안 인증 정보가 있는 IAM 사용자를 생성하는 대신 임시 보안 인증 정보를 사용하는 것이 좋습니다. 의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 의 보안 모범 사례를 IAM IAM참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:user/devops-guru-user-
name"]
            }
        }
    ]
}
```

다른 계정에서 Amazon SNS 주제 추가

다른 계정에서 Amazon SNS 주제에 대한 권한을 구성한 후 해당 Amazon SNS 주제를 DevOpsGuru 알림 설정에 추가할 수 있습니다. AWS CLI 또는 DevOpsGuru 콘솔을 사용하여 Amazon SNS 주제를 추가할 수 있습니다.

- 콘솔을 사용하는 경우 다른 계정의 SNS 주제를 사용하려면 주제 사용 옵션을 선택하여 기존 주제를 ARN 지정해야 합니다.
- AWS CLI 작업 를 사용할 때는 `NotificationChannelConfig` 객체 `TopicArn` 내에서 를 지정add-notification-channel해야 합니다.

콘솔을 사용하여 다른 계정에서 Amazon SNS 주제 추가

1. 에서 Amazon DevOpsGuru 콘솔을 엽니다https://console.aws.amazon.com/devops-guru/.
2. 콘솔을 열고 탐색 창에서 설정을 선택합니다.
3. 알림 섹션으로 이동하여 편집을 선택합니다.
4. SNS 주제 추가를 선택합니다.
5. SNS 주제 사용을 선택하여 기존 주제를 ARN 지정합니다.
6. 사용하려는 Amazon SNS 주제ARN의 를 입력합니다. 정책을 연결하여 이 주제에 대한 권한을 이미 구성했어야 합니다.
7. (선택 사항) 알림 빈도 설정을 편집하려면 알림 구성을 선택합니다.
8. 저장(Save)을 선택합니다.

알림 설정에 Amazon SNS 주제를 추가한 후 DevOpsGuru는 해당 주제를 사용하여 새 인사이트가 생성될 때와 같은 중요한 이벤트를 알립니다.

알림 채널로 Amazon SNS 정책 업데이트(권장)

주제를 추가한 후에는 주제를 포함하는 DevOpsGuru 알림 채널에 대한 권한만 지정하여 정책을 더 안전하게 만드는 것이 좋습니다.

알림 채널로 Amazon SNS 주제 정책 업데이트(권장)

1. 알림을 보내려는 계정에서 `list-notification-channels` DevOpsGuru AWS CLI 명령을 실행합니다.

```
aws devops-guru list-notification-channels
```

2. `list-notification-channels` 응답에서 Amazon SNS 주제의 가 포함된 채널 ID를 기록해 둡니다ARN. 채널 ID는 guid입니다.

   예를 들어 다음 응답에서 를 사용하는 주제의 채널 ID는 ARN`arn:aws:sns:`*`region-id`*`:`*`111122223333`*`:`*`topic-name`*입니다. *`e89be5f7-989d-4c4c-b1fe-e7145037e531`*

```
{
  "Channels": [
    {
      "Id": "e89be5f7-989d-4c4c-b1fe-e7145037e531",
      "Config": {
      "Sns": {
          "TopicArn": "arn:aws:sns:region-id:111122223333:topic-name"
        },
      "Filters": {
          "MessageTypes": ["CLOSED_INSIGHT", "NEW_INSIGHT", "SEVERITY_UPGRADED"],
          "Severities": ["HIGH", "MEDIUM"]
        }
      }
    }
  ]
}
```

3. the section called “다른 계정의 Amazon SNS 주제에 대한 권한 구성”에서 주제 소유자 ID를 사용하여 다른 계정에서 만든 정책으로 이동합니다. 정책의 `Condition` 문장에 `SourceArn`을 지정하는 줄을 추가하십시오. 에는 리전 ID(예: `us-east-1`), 주제 발신자의 AWS 계정 번호, 메모한 채널 ID가 ARN 포함됩니다.

   업데이트된 `Condition` 문장은 다음과 같습니다.

```
"Condition" : {
  "StringEquals" : {
    "AWS:SourceArn": "arn:aws:devops-guru:us-
east-1:111122223333:channel/e89be5f7-989d-4c4c-b1fe-e7145037e531",
    "AWS:SourceAccount": "111122223333"
   }
 }
```

`AddNotificationChannel` 가 SNS 주제를 추가할 수 없는 경우 IAM 정책에 다음 권한이 있는지 확인합니다.

```
{
     "Version": "2012-10-17",
     "Statement": [{
           "Sid": "DevOpsGuruTopicPermissions",
           "Effect": "Allow",
           "Action": [
                 "sns:CreateTopic",
                 "sns:GetTopicAttributes",
                 "sns:SetTopicAttributes",
                 "sns:Publish"
           ],
           "Resource": "arn:aws:sns:region-id:account-id:my-topic-name"
     }]
}
```

AWS KMS암호화 Amazon SNS 주제에 대한 권한

지정한 Amazon SNS 주제는 에 의해 암호화될 수 있습니다 AWS Key Management Service. DevOpsGuru가 암호화된 주제로 작업할 수 있도록 하려면 먼저 를 생성한 AWS KMS key 다음 KMS 키 정책에 다음 문을 추가해야 합니다. 자세한 내용은 사용 설명서AWS의 , 키 식별자(), Amazon Simple Notification Service 개발자 안내서의 데이터 암호화SNS를 사용하여 Amazon에 게시된 메시지 암호화KMS를 참조하세요. KeyId AWS KMS https://docs.aws.amazon.com/sns/latest/dg/sns-data-encryption.html

```
{
  "Version": "2012-10-17",
  "Id": "your-kms-key-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

> **Note**
>
> DevOpsGuru는 현재 단일 계정 내에서 사용할 암호화된 주제를 지원합니다. 여러 계정에서 암호화된 주제를 사용하는 것은 현재는 지원하지 않습니다.

Amazon DevOpsGuru 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 DevOpsGuru 및 에서 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결할 수 있습니다IAM.

주제

- DevOpsGuru에서 작업을 수행할 권한이 없습니다.
- 사용자에게 프로그래밍 방식으로 액세스 권한을 부여하고 싶습니다.
- iam을 수행할 권한이 없습니다.PassRole
- 내 AWS 계정 외부의 사람들이 내 DevOpsGuru 리소스에 액세스하도록 허용하고 싶습니다.

DevOpsGuru에서 작업을 수행할 권한이 없습니다.

에 작업을 수행할 권한이 없다고 AWS Management Console 표시되면 관리자에게 문의하여 지원을 받아야 합니다.

다음 예제 오류는 `mateojackson` 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `aws:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

이 경우 Mateo는 *`my-example-widget`* 작업을 사용하여 `aws:`*`GetWidget`* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

사용자에게 프로그래밍 방식으로 액세스 권한을 부여하고 싶습니다.

사용자는 AWS 외부에서 와 상호 작용하려는 경우 프로그래밍 방식으로 액세스해야 합니다 AWS Management Console. 프로그래밍 방식 액세스를 부여하는 방법은 에 액세스하는 사용자 유형에 따라 다릅니다 AWS.

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
작업 인력 ID (IAMID 센터에서 관리하는 사용자)	임시 자격 증명을 사용하여 AWS CLI AWS SDKs, 또는 에 대한 프로그래밍 요청에 서명합니다 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 의 경우 AWS Command Line Interface 사용 설명서의 AWS CLI 를 사용하도록 구성을 AWS IAM Identity Center AWS CLI참조하세요. • AWS SDKs, 도구 및 의 경우 AWS SDKs 및 도구 참조 가이드의 IAM Identity Center 인증을 AWS APIs참조하세요.
IAM	임시 자격 증명을 사용하여 AWS CLI AWS SDKs, 또는 에 대한 프로그래밍 요청에 서명합니다 AWS APIs.	IAM 사용 설명서의 AWS 리소스와 함께 임시 자격 증명 사용의 지침을 따릅니다.
IAM	(권장되지 않음) 장기 보안 인증 정보를 사용하여 AWS CLI AWS SDKs, 또는 에 대한 프로그래밍 요청에 서명합니다 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 의 경우 AWS Command Line Interface 사용 설명서의 IAM 사용자 자격 증명을 사용하여 인증을 AWS CLI참조하세요.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
		• 및 도구에 대한 AWS SDKs 자세한 내용은 AWS SDKs 및 도구 참조 가이드의 장기 보안 인증 정보를 사용하여 인증을 참조하세요. • 의 경우 IAM 사용 설명서의 IAM 사용자에 대한 액세스 키 관리를 AWS APIs참조하세요.

iam을 수행할 권한이 없습니다.PassRole

`iam:PassRole` 작업을 수행할 권한이 없다는 오류가 발생하면 DevOpsGuru에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있도록 AWS 서비스 허용합니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 이름이 인 IAM 사용자가 콘솔을 사용하여 DevOpsGuru에서 작업을 수행하려고 `marymajor` 할 때 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:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사람들이 내 DevOpsGuru 리소스에 액세스하도록 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(ACLs)을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- DevOpsGuru가 이러한 기능을 지원하는지 알아보려면 섹션을 참조하세요Amazon DevOpsGuru의 작동 방식 IAM.
- 소유 AWS 계정 한 의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유 AWS 계정 한 다른 의 IAM 사용자에게 액세스 권한 제공을 참조하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유 에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- 자격 증명 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부 인증 사용자(자격 증명 페더레이션)에 대한 액세스 제공을 참조하세요.
- 교차 계정 액세스를 위한 역할 및 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 에서 교차 계정 리소스 액세스를 IAM 참조하세요.

DevOpsGuru 로깅 및 모니터링

모니터링은 DevOpsGuru 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS 는 DevOpsGuru를 감시하고, 문제가 있을 때 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon CloudWatch은 AWS 리소스와 실행 중인 애플리케이션을 AWS 실시간으로 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적하고 필요한 경우 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서 섹션을 참조하세요.
- AWS CloudTrail 는 AWS 계정에서 직접 또는 계정을 대신하여 수행한 API 통화 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전달합니다. 어떤 사용자 및 계정이 AWS 를 호출했는지 어떤 소스 IP 주소에 호출이 이루어졌는지 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

주제

- Amazon을 사용한 DevOpsGuru 모니터링 CloudWatch

- 를 사용하여 Amazon DevOpsGuru API 호출 로깅 AWS CloudTrail

Amazon을 사용한 DevOpsGuru 모니터링 CloudWatch

원시 데이터를 수집 CloudWatch하여 읽기 가능한 실시간에 가까운 지표로 처리하는 를 사용하여 DevOpsGuru를 모니터링할 수 있습니다. 이러한 통계는 15개월간 보관되므로 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. 특정 임계값을 주시하다가 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서 섹션을 참조하세요.

DevOpsGuru의 경우 DevOpsGuru 사용량에 대한 인사이트 및 지표를 추적할 수 있습니다. 운영 솔루션에 비정상적인 동작이 발생하고 있는지 판단하는 `Insights`데 도움이 될 수 있도록 생성된 많은 수의 인사이트를 살펴보는 것도 좋습니다. 또는 DevOpsGuru 사용량을 관찰하여 비용을 추적하는 데 도움이 될 수 있습니다.

DevOpsGuru 서비스는 `AWS/DevOps-Guru` 네임스페이스에 다음 지표를 보고합니다.

주제

- 인사이트 지표
- DevOpsGuru 사용 지표

인사이트 지표

CloudWatch 를 사용하여 지표를 추적하여 계정에 생성된 인사이트 수를 표시할 수 있습니다 AWS . `Type` 차원을 지정하여 `proactive` 또는 `reactive` 인사이트를 추적할 수 있습니다. 모든 인사이트를 추적하려면 차원을 지정하지 마십시오.

지표

지표	설명
`Insight`	AWS 계정에서 생성된 인사이트 수입니다. 유효한 차원: `Type` 유효한 통계: Sum, Sample Count 단위: 개

DevOpsGuru 지표에는 다음 `Insight` 차원이 지원됩니다.

측정기준

차원	설명
`Type`	이 유형은 인사이트 유형입니다. 모든 인사이트를 추적하려면 `Insights` 지표의 차원을 지정하지 마십시오. 유효 값은 `proactive` , `reactive`입니다.

DevOpsGuru 사용 지표

CloudWatch 를 사용하여 Amazon DevOpsGuru 사용량을 추적할 수 있습니다.

지표

지표	설명
`CallCount`	다음 DevOpsGuru 메서드 중 하나에 의해 수행된 통화 수입니다. • ListInsights • ListAnomaliesForInsight • ListRecommendations • ListEvents • SearchInsights • DescribeInsight • DescribeAnomaly 유효한 차원: `Service`, `Class`, `Type`, `Resource`

지표	설명
	유효한 통계: Sum, Sample Count 단위: 개

DevOpsGuru 사용 지표에는 다음 차원이 지원됩니다.

측정기준

차원	설명
`Service`	리소스가 포함된 AWS 서비스의 이름입니다. 예를 들어 DevOpsGuru의 경우 이 값은 입니다`DevOps-Guru` .
`Class`	추적되는 리소스의 클래스입니다. DevOpsGuru는 이 차원을 값과 함께 사용합니다`None`.
`Type`	추적되는 리소스 유형입니다. DevOpsGuru는 이 차원을 값과 함께 사용합니다`API`.
`Resource`	DevOpsGuru 작업의 이름입니다. 유효한 값은 `ListInsights` , `ListAnomaliesForInsight` , `ListRecommendations` , `ListEvents` , `SearchInsights` , `DescribeInsight` , `DescribeAnomaly` 입니다.

를 사용하여 Amazon DevOpsGuru API 호출 로깅 AWS CloudTrail

Amazon DevOpsGuru는 DevOpsGuru. CloudTrail captures에서 사용자 AWS CloudTrail, 역할 또는 서비스가 DevOpsGuru를 이벤트로 API 호출하는 작업에 대한 레코드를 제공하는 AWS 서비스인 와 통합됩니다. 캡처된 호출에는 DevOpsGuru 콘솔의 호출과 DevOpsGuru API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하는 경우 DevOpsGuru에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록 에서 최신 이벤트를 볼 수 있습니다. 에서 수집한 정보를 사용하여 DevOpsGuru에 수행된 요청 CloudTrail, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

에 대한 자세한 내용은 AWS CloudTrail 사용 설명서 섹션을 CloudTrail참조하세요.

DevOps의 Guru 정보 CloudTrail

CloudTrail 는 AWS 계정을 생성할 때 계정에서 활성화됩니다. DevOpsGuru에서 활동이 발생하면 해당 활동은 CloudTrail 이벤트 기록 의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록을 사용하여 CloudTrail 이벤트 보기를 참조하세요.

DevOpsGuru에 대한 이벤트를 포함하여 AWS 계정의 이벤트에 대한 지속적인 기록을 위해 추적을 생성합니다. 추적을 사용하면 CloudTrail 가 Amazon S3 버킷에 로그 파일을 전달할 수 있습니다. 기본적으로 콘솔에서 추적을 생성하면 추적이 모든 AWS 리전에 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 기록하고 지정한 Amazon S3 버킷에 로그 파일을 전달합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 작업하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

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

DevOpsGuru는 모든 작업을 CloudTrail 로그 파일의 이벤트로 로깅하는 것을 지원합니다. 자세한 내용은 DevOpsGuru API 참조의 작업을 참조하세요.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 사용자 자격 증명으로 했는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

DevOpsGuru 로그 파일 항목 이해

추적은 사용자가 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있도록 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함됩니다. 이벤트는 모든 소스의 단일 요청을 나

타내며 요청된 작업, 작업 날짜 및 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 정렬된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

다음 예제에서는 `UpdateResourceCollection` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAEXAMPLE:TestSession",
    "arn": "arn:aws:sts::123456789012:assumed-role/TestRole/TestSession",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/TestRole",
        "accountId": "123456789012",
        "userName": "sample-user-name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-12-03T15:29:51Z"
      }
    }
  },
  "eventTime": "2020-12-01T16:14:31Z",
  "eventSource": "devops-guru.amazonaws.com",
  "eventName": "UpdateResourceCollection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "sample-ip-address",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.901
 Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
  "requestParameters": {
    "Action": "REMOVE",
    "ResourceCollection": {
      "CloudFormation": {
        "StackNames": [
          "*"
```

```
        ]
      }
    }
  },
  "responseElements": null,
  "requestID": " cb8c167e-EXAMPLE ",
  "eventID": " e3c6f4ce-EXAMPLE ",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

DevOpsGuru 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

Amazon DevOpsGuru 를 호출할 때 VPC 엔드포인트를 사용할 수 있습니다APIs. VPC 엔드포인트를 사용하면 에 포함되어 VPC 있고 인터넷에 액세스하지 않기 때문에 API 통화가 더 안전합니다. 자세한 내용은 Amazon DevOpsGuru API 참조의 작업을 참조하세요.

인터페이스 VPC 엔드포인트 를 생성하여 VPC 와 DevOpsGuru 간에 프라이빗 연결을 설정합니다. 인터페이스 엔드포인트는 인터넷 게이트웨이AWS PrivateLink, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 APIs 없이 DevOpsGuru에 비공개로 액세스할 수 있는 기술인 로 구동됩니다. 의 인스턴스는 DevOpsGuru 와 통신하는 데 퍼블릭 IP 주소가 필요하지 VPC 않습니다APIs. VPC 와 DevOpsGuru 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 탄력적 네트워크 인터페이스로 표현됩니다.

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.

DevOpsGuru VPC 엔드포인트에 대한 고려 사항

DevOpsGuru에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 속성 및 제한을 검토해야 합니다.

DevOpsGuru는 에서 모든 API 작업에 대한 호출을 지원합니다VPC.

DevOpsGuru용 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 DevOpsGuru 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 DevOpsGuru용 VPC 엔드포인트를 생성합니다.

- com.amazonaws.*region*.devops-guru

엔드포인트에 DNS 대해 프라이빗을 활성화하는 경우 리전의 기본 DNS 이름, 예를 들어 를 사용하여 DevOpsGuru에 API 요청할 수 있습니다`devops-guru.us-east-1.amazonaws.com`.

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트를 통한 서비스 액세스를 참조하세요.

DevOpsGuru에 대한 VPC 엔드포인트 정책 생성

DevOpsGuru에 대한 액세스를 제어하는 엔드포인트에 VPC 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 사용하여 서비스에 대한 액세스 제어를 참조하세요.

예: DevOpsGuru 작업에 대한 VPC 엔드포인트 정책

다음은 DevOpsGuru에 대한 엔드포인트 정책의 예입니다. 엔드포인트에 연결되면 이 정책은 모든 리소스의 모든 보안 주체에 대해 나열된 DevOpsGuru 작업에 대한 액세스 권한을 부여합니다.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
```

```
            "devops-guru:AddNotificationChannel",
            "devops-guru:ListInsights",
            "devops-guru:ListRecommendations"
         ],
         "Resource":"*"
      }
   ]
}
```

DevOpsGuru의 인프라 보안

관리형 서비스인 Amazon DevOpsGuru는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및 가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안 섹션을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 DevOpsGuru에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- DHE (Ephemeral Diffie-HellmanPFS) 또는 (Elliptic Curve Ephemeral Diffie-Hellman)과 같은 완벽한 순방향 보안ECDHE()이 포함된 Cipher 제품군입니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 IAM 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

Amazon DevOpsGuru의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 구축됩니다. AWS 리전은 지연 시간이 짧고 처리량이 높고 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. DevOpsGuru는 여러 가용 영역에서 작동하며 Amazon S3 및 Amazon DynamoDB 에 아티팩트 데이터 및 메타데이터를 저장합니다. 암호화된 데이터가 여러 시설과 각 시설의 여러 디바이스에 중복 저장되어 가용성과 내구성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라 섹션을 참조하세요.

Amazon DevOps Guruu에 사용되는 할당량 및 제한

다음 표에는 Amazon DevOps Guru의 현재 할당량이 나와 있습니다. 이 할당량은 각 계정의 AWS 지원 지역별 AWS 할당량입니다.

알림

한 번에 지정할 수 있는 Amazon Simple Notification Service 주제의 최대 수	2

AWS CloudFormation 스택

지정할 수 있는 AWS CloudFormation 최대 스택 수	1000

DevOps Guru 리소스 모니터링 제한

리소스 설명	한도	높일 수 있음
Amazon Simple Queue Service(Amazon SQS) 대기열을 모니터링하기 위한 기본 제한	100*	예**

*2023년 6월 29일 또는 그 이후에 생성된 새 DevOps Guru 계정 및 Amazon SQS 대기열이 100개 미만인 기존 계정과 같은 날짜에 활성화된 계정에 해당합니다.

**이 제한 변경을 요청하려면 AWS Supporthttps://aws.amazon.com/contact-us으로 문의하십시오. Amazon SQS 대기열 모니터링 제한을 100, 500, 1,000, 5,000 또는 10,000으로 요청할 수 있습니다.

API 생성, 배포 및 관리를 위한 DevOps Guru 할당량

DevOps Guru에서 AWS CLI, API Gateway 콘솔 또는 API Gateway REST API 및 SDK를 사용하여 API를 생성, 배포 및 관리하는 경우 다음과 같이 고정된 할당량이 적용됩니다.

모든 DevOps Guru API 목록은 Amazon DevOps Guru 작업을 참조하십시오.

기본 할당량	높일 수 있음	
하나의 계정에 대해 1초당 20개의 요청	예	

Amazon DevOps Guru 문서 기록

다음 표는 본 DevOps Guru 릴리스 관련 설명서를 소개합니다.

- API 버전: 최신
- 최종 설명서 업데이트: 2023년 8월 9일

변경 사항	설명	날짜
관리형 정책 업데이트	Amazon SNS 구독 및 구독 목록 액세스가 `AmazonDevOpsGuruConsoleFullAccess` 정책에 추가되었습니다. 구독 목록 액세스도 `AmazonDevOpsGuruReadOnlyAccess` 정책에 추가되었습니다. 자세한 내용은 Amazon DevOps Guru에 대한 자격 증명 기반 정책을 참조하세요.	2023년 8월 9일
고객 관리형 암호화 키	이제 DevOps Guru는 AWS KMS을(를) 사용하여 고객 관리형 키를 통한 암호화를 지원합니다. 자세한 내용은 DevOps Guru의 데이터 보호 단원을 참조하십시오.	2023년 7월 5일
RDS용 DevOps Guru는 RDS PostgreSQL을 지원합니다	RDS용 DevOps Guru는 PostgreSQL 데이터베이스에서 성능 병목 현상 및 기타 인사이트를 감지할 수 있습니다. 자세한 내용은 DevOps Guru for RDS의 이점을 참조하세요.	2023년 3월 30일

DevOps Guru for RDS에서 사전 예방 인사이트 지원	DevOps Guru for RDS는 Aurora 데이터베이스에서 문제가 발생할 것으로 예측되기 전에 문제를 해결하는 데 도움이 되는 권장 사항과 함께 사전 예방 인사이트를 게시합니다. 자세한 내용은 DevOps Guru for RDS 이상을 참조하세요.	2023년 2월 28일
분석된 리소스 페이지	DevOps Guru 콘솔의 새 페이지에는 귀하의 계정에서 DevOps Guru가 분석한 리소스가 나열됩니다. 더 자세한 내용은 DevOps Guru가 분석한 리소스 보기를 참고하십시오.	2022년 10월 20일
새 알림 구성 설정	이제 모든 알림을 수신할지 또는 특정 심각도 및 이벤트에 대한 알림만 수신할지 선택할 수 있습니다. 자세한 내용은 Amazon SNS 알림 설정업데이트 업데이트를 참조하십시오.	2022년 9월 30일
관리형 정책에 로그 이상 항목 분석 추가	DevOps Guru의 AWS 관리형 정책이 IAM 콘솔에서 업데이트되어 CloudWatch 작업 `FilterLogEvents` 에 대한 액세스를 지원합니다. 더 자세한 내용은 AWS 관리형 정책 및 서비스 연결 역할에 대한 DevOps Guru 업데이트를 참고하십시오.	2022년 8월 30일

로그 이상 항목 분석 추가됨	DevOps Guru 콘솔에서 인사이트와 관련된 로그 그룹에 대한 자세한 정보를 볼 수 있습니다. 또한, CloudWatch 로그 및 스트림을 설명하는 데 사용할 수 있는 확장된 서비스 연결 역할도 있습니다. 더 자세한 내용은 DevOps Guru 콘솔에서 인사이트 이해 및 AWS 관리형 정책 및 서비스 연결 역할에 대한 DevOps Guru 업데이트를 참고하십시오.	2022년 7월 12일
CodeGuru Profiler 통합	이제 DevOps Guru는 EventBridge 관리형 규칙이 포함된 Amazon CodeGuru Profiler와 통합됩니다. CodeGuru Profiler의 각 인바운드 이벤트는 사전 예방적 이상 항목 보고서입니다. 자세한 내용은 CodeGuru Profiler 와 통합을 참조하세요.	2022년 3월 7일
관리형 업데이트 서비스 연결 역할 업데이트	IAM 콘솔에서 사용 가능한 확장된 정책. 이번 변경을 통해 DevOps Guru는 Amazon Relational Database Service(Amazon RDS)와의 향상된 통합 기능을 지원할 수 있게 되었습니다. 더 자세한 내용은 DevOps Guru용 서비스 연결 역할 및 AWS 관리형(미리 정의된) 정책 사용을 참고하십시오.	2021년 12월 21일

새 관리형 정책 추가됨	`AmazonDevOpsGuruConsoleFullAccess` 정책이 추가되었습니다. 자세한 내용은 Amazon DevOps Guru에 대한 자격 증명 기반 정책을 참조하세요.	2021년 12월 6일
AWS 태그로 애플리케이션 정의 지원	이제 AWS 태그를 사용하여 DevOps Guru가 분석할 리소스를 파악하고, 애플리케이션의 리소스를 파악하고, 콘솔에서 인사이트를 필터링할 수 있습니다. 더 자세한 내용은 태그를 사용하여 애플리케이션의 리소스 파악을 참고하십시오.	2021년 12월 1일
관리형 업데이트 서비스 연결 역할 업데이트	IAM 콘솔에서 사용 가능한 확장된 정책. 이번 변경을 통해 DevOps Guru는 Amazon Relational Database Service(Amazon RDS)와의 향상된 통합 기능을 지원할 수 있게 되었습니다. 더 자세한 내용은 DevOps Guru용 서비스 연결 역할 및 AWS 관리형(미리 정의된) 정책 사용을 참고하십시오.	2021년 12월 1일
Amazon RDS 지원 사항	이제 DevOps Guru는 귀하의 애플리케이션에서 Amazon Relational Database Service(Amazon RDS) 리소스에 대한 종합 분석 및 인사이트를 제공합니다. 더 자세한 내용은 Amazon RDS용 DevOps Guru에서 이상 항목 처리를 참고하십시오.	2021년 12월 1일

Amazon EventBridge 통합	이제 DevOps Guru는 EventBridge와 통합되어 DevOps Guru 인사이트와 관련된 특정 이벤트를 알려줍니다. 자세한 내용은 EventBridge로 작업 섹션을 참조하세요.	2021년 11월 18일
AWS 관리형 정책 추가됨	새로운 AWS 관리형 정책이 추가되었습니다. 이 `AmazonDevOpsGuruOrganizationsAccess` 정책은 조직 내 DevOps Guru에 대한 액세스를 제공합니다. 자세한 내용은 자격 증명 기반 정책 섹션을 참조하세요.	2021년 11월 16일
서비스 연결 역할 정책 업데이트	IAM 콘솔에서 사용 가능한 확장된 정책 이번 변경을 통해 DevOps Guru는 다중 계정 보기를 지원할 수 있게 되었습니다. 자세한 내용은 서비스 연결 역할 사용을 참조하십시오.	2021년 11월 4일
계정 간 지원	이제 조직 내 여러 계정에서 인사이트 및 메트릭을 볼 수 있습니다. 자세한 내용은 Amazon DevOps Guru란 무엇인가를 참조하세요.	2021년 11월 4일
정식 출시 릴리스	이제 Amazon DevOps Guru를 정식 버전 (GA) 으로 사용할 수 있습니다.	2021년 5월 4일

새로운 주제	이제 DevOps Guru의 월별 예상 비용을 생성하여 리소스를 분석할 수 있습니다. 더 자세한 내용은 Amazon DevOps Guru 비용 예측을 참고하십시오.	2021년 4월 27일
VPC 엔드포인트 지원	이제 VPC 엔드포인트를 사용하여 리소스 분석 및 인사이트 생성의 보안을 개선할 수 있습니다. 자세한 내용은 DevOps Guru 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.	2021년 4월 15일
새로운 주제	Amazon CloudWatch를 사용하여 DevOps Guru를 모니터링하는 방법에 대한 새로운 주제가 추가되었습니다. 자세한 내용은 Amazon CloudWatch를 사용하여 DevOps Guru를 모니터링 단원을 참조하십시오.	2020년 12월 11일
프리뷰 릴리스	이 릴리스는 Amazon DevOps Guru 사용 설명서에 대한 미리보기 릴리스입니다.	2020년 12월 1일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하세요.

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