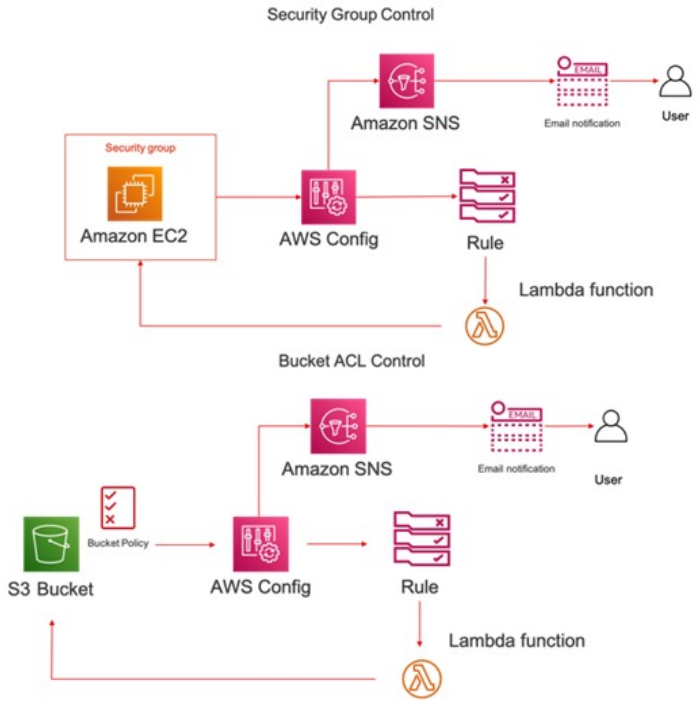
Management & Governance

L조 김현민, 조윤아, 조은비, 한예성

Management and Governance

과거에는 **조직이 빠른 혁신과 비용, 규정 준수 및 보안**의 제어 유지 중 하나를 선택해야 했습니다.
AWS Management and Governance를 사용하는 고객은 혁신과 제어 중 하나를 선택할 필요없이 둘 다 가질 수 있습니다.
AWS 고객은 **비즈니스 민첩성과 거버넌스 제어를 모두 지원**하는 환경을 활성화, **프로비저닝 및 운영**할 수 있습니다.



예) AWS Config Rule을 활용하여 탐지제어를 구현하고, 람다를 사용하여 실시간 교정작업 생성

AWS CloudFormation

AWS Config

AWS SystemsManager

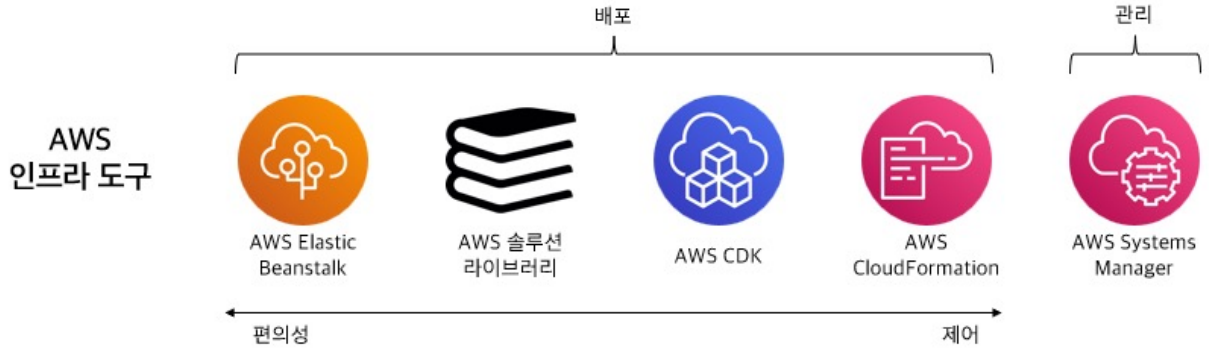
AWS TrustedAdvisor

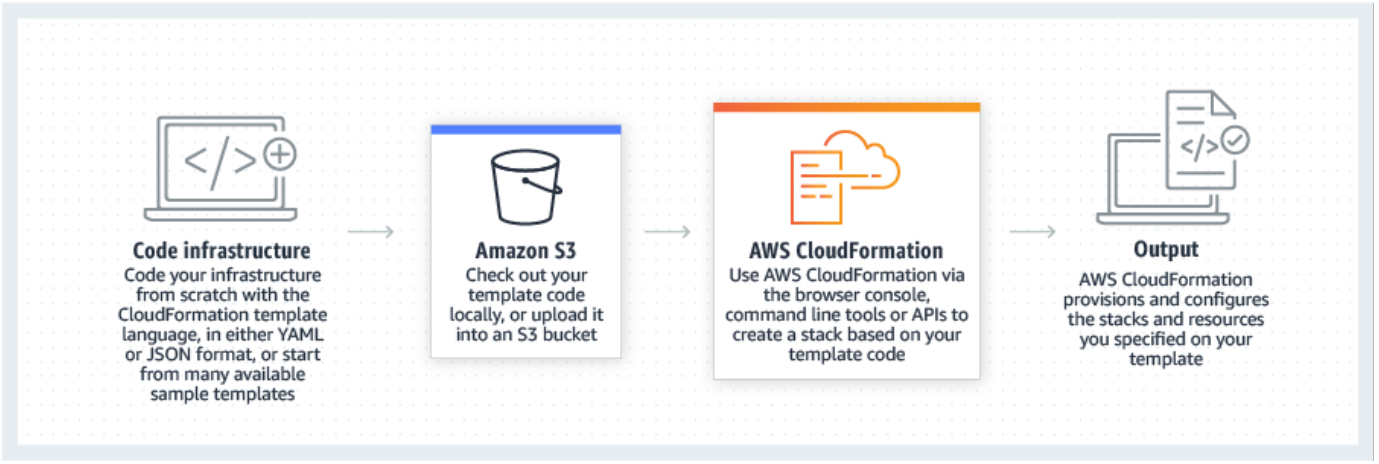
AWS SecretsManager

AWS CloudFormation

AWS CloudFormation

AWS CloudFormation은 AWS 리소스를 모델링, 설정하여 리소스 관리 시간을 줄이고 애플리케이션 개발에 더 많은 시간을 할애할 수 있게 해주는 코드형 인프라(IaC) 도구입니다. **코드형 인프라(Infrastructure as Code: IaC)**는 인프라 구조를 코드로 작성하고 관리하는 방식을 말합니다. 인프라에 속하는 모든 구성 요소를 세부적으로 제어할 수 있고, AWS 리소스를 개별적으로 생성하고 구성할 필요 없이 모든 것을 AWS CloudFormation가 알아서 처리합니다.





서비스 개요

- 사용하려는 AWS 리소스를 **템플릿 파일**로 작성하면 CloudFormation이 이를 분석하여 적절한 AWS 리소스를 생성합니다.
- 해당 리소스는 AWS 서비스로 전송되는 API 호출로 변환되고 **리소스 스택**으로 저장되는 구조를 가지고 있습니다.

서비스 작동 방식

1. CloudFormation 템플릿 생성 (JSON, YAML)
2. 템플릿을 Amazon S3 또는 로컬 환경에 저장
3. 템플릿을 이용하여 리소스 스택 생성

AWS CloudFormation

AWS CloudFormation에서는 템플릿과 스택이라는 용어가 등장합니다.

템플릿은 환경에서 배포할 리소스를 설명하고 정의하는 JSON 또는 YAML 형식의 텍스트 파일입니다. 로컬 또는 Amazon S3 버킷에 저장할 수 있습니다.

스택은 하나의 단위로 관리할 수 있는 AWS 리소스의 모음입니다. 리소스 배포, 삭제 및 실행 중인 스택의 리소스 및 설정을 업데이트할 수 있습니다.

서비스 주요 기능

- 인프라 관리 간소화
- 빠른 속도와 높은 안정성
- 재사용성 – 템플릿을 이용하여 신속하게 인프라 복제
- 교차 스택 참조 지원
- 인프라 변경 사항을 쉽게 제어 및 추적 가능
- Git, Subversion 등 버전 제어 시스템으로 템플릿 관리 가능

서비스 사용 예시

1. **DevOps로 인프라 관리**

   지속적 통합 및 전달(CI/CD) 자동화로 인프라 템플릿을 자동화하고 테스트/배포할 수 있습니다.

2. **프로덕션 스택 크기 조정**

   단일 Amazon EC2 인스턴스부터 복잡한 다중 리전 애플리케이션까지 실행할 수 있습니다.

3. **모범 사례 공유**

   Amazon VPC 서브넷 또는 프로비저닝 서비스(AWS OpsWorks, Amazon ECS)를 손쉽게 정의할 수 있습니다.

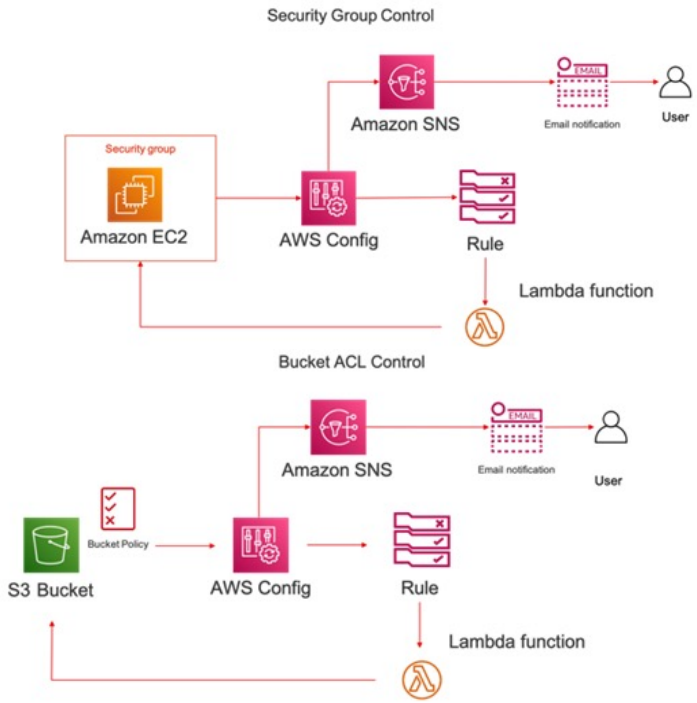
템플릿 JSON 예시

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Description" : "A sample template",
  "Resources" : {
    "MyEC2Instance" : {
      "Type" : "AWS::EC2::Instance",
      "Properties" : {
        "ImageId" : "ami-0ff8a91507f77f867",
        "InstanceType" : "t2.micro",
        "KeyName" : "testkey",
        "BlockDeviceMappings" : [
          {
            "DeviceName" : "/dev/sdm",
            "Ebs" : {
              "VolumeType" : "io1",
              "Iops" : 200,
              "DeleteOnTermination" : false,
              "VolumeSize" : 20
            }
          ...
```

AWS Config

AWS Config

AWS Config는 아마존 웹 서비스에서 제공하는 서비스로 사용자가 **AWS 리소스의 구성**을 볼 수 있으며, 이를 통해 **AWS 리소스 간의 관계 및 과거 구성 방식**을 볼 수 있습니다. EC2 인스턴스, EBS 볼륨, 보안 그룹 및 VPC와 같은 다양한 유형의 AWS 리소스를 지원합니다. 이 서비스에는 **리소스 관리, 규칙 및 준수 팩, 집계기 및 고급 쿼리**와 같은 기능이 포함됩니다. 이를 통해 사용자는 **리소스를 모니터링 및 관리**하고, **컴플라이언스를 평가**하며, **문제를 해결**하고, **보안 분석을 수행**할 수 있습니다.



예) AWS Config Rule을 활용하여 탐지제어를 구현하고, 람다를 사용하여 실시간 교정작업 생성

Resource management
AWS Config에서 기록할 리소스 유형을 지정
요청 및 구성 기록에 따라 구성 스냅샷을 받도록 Amazon S3 버킷을 설정
구성 스트림 알림을 보내도록 Amazon SNS를 설정
AWS Config에 Amazon S3 버킷 및 Amazon SNS 항목에 액세스하는 데 필요한 사용 권한을 부여

Rules and conformance packs
AWS Config에서 기록된 리소스 유형에 대한 컴플라이언스 정보를 평가하는 데 사용할 규칙을 지정
준수 팩을 사용하거나 AWS 계정에서 단일 엔티티로 배포하고 모니터링할 수 있는 AWS Config 규칙 및 업데이트 적용 작업 모음을 사용

Aggregators
집계 도구를 사용하여 리소스 인벤토리 및 규정 준수에 대한 중앙 집중식 보기를 얻을 수 있음.

Advanced queries
샘플 쿼리 중 하나를 사용하거나 AWS 리소스의 구성 스키마를 참조하여 자신의 쿼리를 작성 가능

ex)

```
SELECT configuration WHERE configuration.configRuleList.complianceType = 'non_compliant' AND configuration.configRuleList.configRuleName = ‘A’
```

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

AWS Config

리소스 관리

리소스 구성을 보다 효과적으로 제어하고 리소스 구성 오류를 감지하려면 언제든지 어떤 리소스가 존재하고 이러한 리소스가 구성되는 방식을 세부적으로 파악해야 합니다. **AWS Config를 사용하면 각 리소스에 대한 호출을 폴링하여 이러한 변경 사항을 모니터링할 필요 없이 리소스가 생성, 수정 또는 삭제될 때마다 사용자에게 알릴 수 있습니다.** AWS Config 규칙을 사용하여 AWS 리소스의 구성 설정을 평가할 수 있습니다. **AWS Config가 리소스가 규칙 중 하나의 조건을 위반하는 것을 감지하면 AWS Config는 리소스를 비준수로 플래그 지정하고 알림을 보냅니다.** AWS Config는 리소스가 생성, 변경 또는 삭제될 때 지속적으로 평가합니다.

감사 및 규정 준수

내부 정책 및 모범 사례 준수를 보장하기 위해 빈번한 감사가 필요한 데이터를 사용하고 있을 수 있습니다. 규정 준수를 입증하려면 리소스의 기록 구성에 액세스해야 합니다. 이 정보는 **AWS Config에서 제공**합니다.

구성 변경 관리 및 문제 해결

서로 종속된 여러 AWS 리소스를 사용하는 경우 한 리소스의 구성이 변경되면 관련 리소스에 의도하지 않은 결과가 발생할 수 있습니다**. AWS Config을 사용하면 수정하려는 리소스가 다른 리소스와 어떻게 관련되어 있는지 확인하고 변경 사항의 영향을 평가할 수 있습니다.** 또한 AWS Config에서 제공하는 리소스의 기록 구성을 사용하여 문제를 해결하고 문제 리소스의 마지막으로 성공한 구성에 액세스할 수 있습니다.

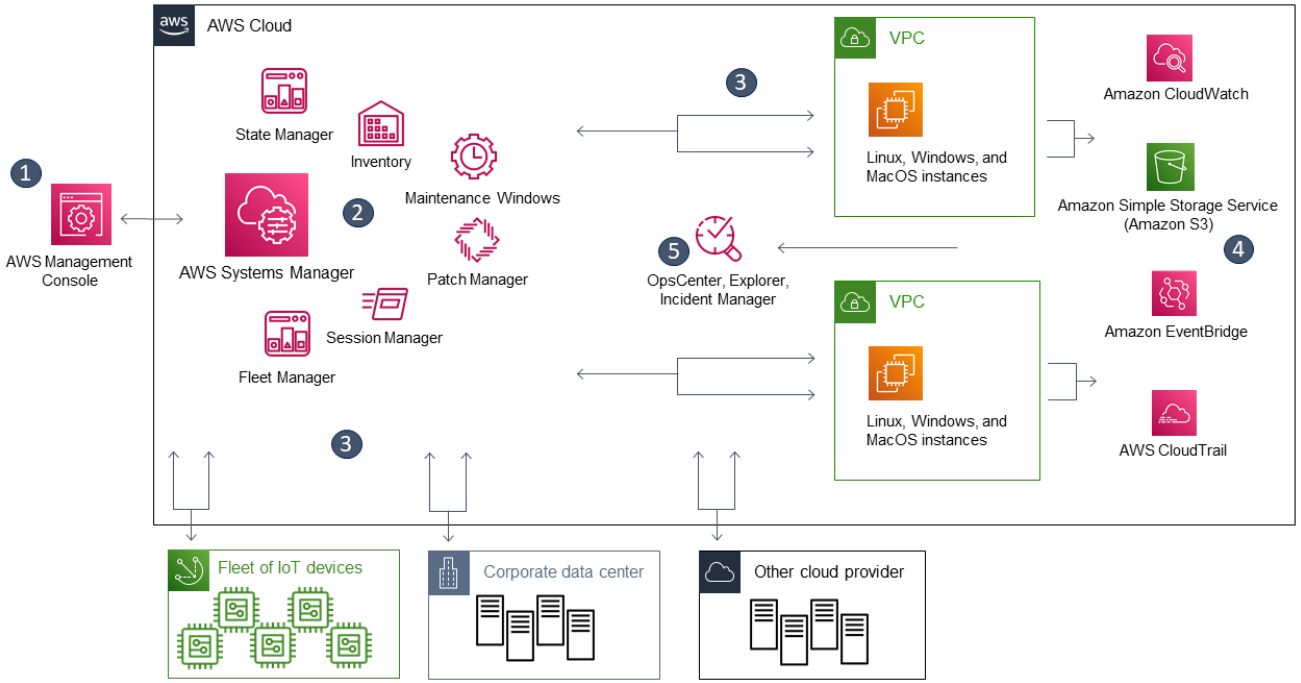
보안 분석

잠재적인 보안 취약성을 분석하려면 사용자에게 부여된 AWS IAM(Identity and Access Management) 사용 권한 또는 리소스에 대한 액세스를 제어하는 Amazon EC2 Security Group 규칙과 같은 AWS 리소스 구성에 대한 자세한 기록 정보가 필요합니다. **AWS Config를 사용하여 AWS Config이 기록되는 동안 언제든지 사용자, 그룹 또는 역할에 할당된 IAM 정책을 볼 수 있습니다**. 이 정보는 **특정 시간에 사용자에게 속했던 사용 권한을 확인하는** 데 도움이 될 수 있습니다. 예를 들어 2015년 1월 1일에 John Doe 사용자에게 Amazon VPC 설정을 수정할 수 있는 사용 권한이 있는지 여부를 확인할 수 있습니다. 또한 AWS Config를 사용하여 특정 시간에 열려 있던 포트 규칙을 포함하여 EC2 Security Group의 구성을 볼 수 있습니다. 이 정보는 보안 그룹이 특정 포트로 들어오는 TCP 트래픽을 차단했는지 여부를 확인하는 데 도움이 될 수 있습니다.

AWS SystemsManager

AWS SystemsManager

AWS 클라우드에서 실행되는 **애플리케이션 및 인프라를 관리**하는 데 도움이 되는 **기능 모음**입니다.
애플리케이션 및 **리소스 관리를 간소화하고, 운영 문제를 감지하고 해결하는 시간을 단축**하며,
AWS 인프라를 규모에 따라 **안전하게 운영 및 관리**하는 데 도움이 됩니다.



① Systems Manager 액세스
② Systems Manager 기능 선택
③ 작업 수행 권한 확인 및 처리
④ 상태 세부 정보 보고
⑤ Systems Manager 운영 관리 기능

AWS SystemsManager

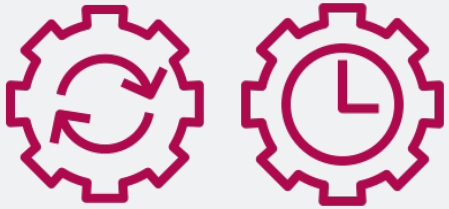
운영 관리

OpsCenter, Explorer,
Incident Manager

애플리케이션 관리

Application Manager,
AppConfig, Parameter Store

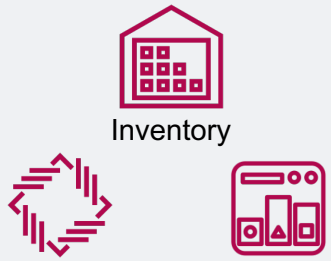
변경 관리



Automation

Maintenance
Windows

노드 관리



Patch Manager

State Manager

운영 데이터의 중앙 집중화

Amazion CloudWatch, AWS CloudTrail 및 AWS Config와 같은 AWS 서비스와 서드 파티 도구 전체에서 실행 가능한 인사이트를 얻고 단일 콘솔에서 데이터를 집계합니다.

애플리케이션 문제를 자동으로 해결

연결된 AWS 리소스 그룹 전체에서 운영 데이터를 사용하여 애플리케이션을 손쉽게 관리하고 문제를 빠르게 식별합니다.

모범 사례 구현

패치 적용 및 리소스 변경과 같은 사전 예방적 프로세스와 사후 대응적 프로세스를 자동화하여 운영 문제가 사용자에게 영향을 미치기 전에 빠르게 진단하고 해결합니다.

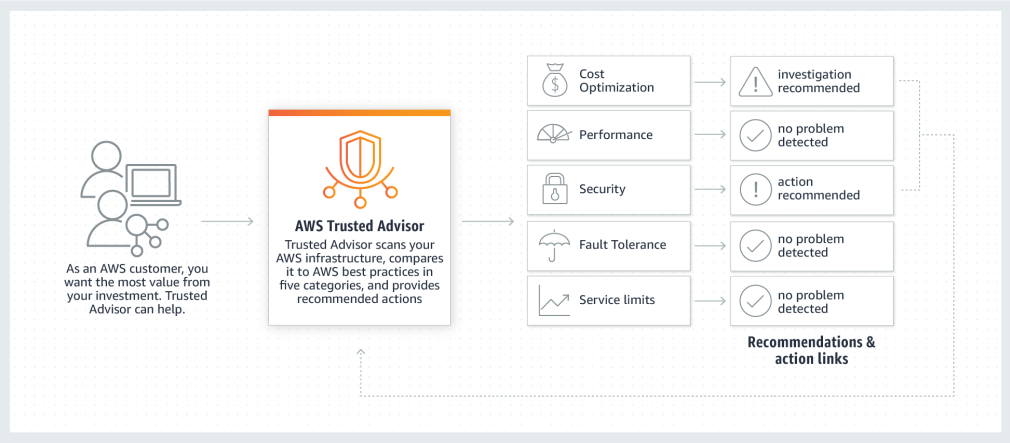
보안 이벤트 해결

보안 및 규정 준수 프로필을 조정하고 보안 이벤트를 추후 분석하여 향후 재발을 방지합니다

AWS
Trusted Advisor

AWS Trusted Advisor

AWS Trusted Advisor는 **AWS 환경을 검사**하고 **비용 절감, 시스템 가용성 및 성능 향상 또는 보안 격차 해소를 위한 권장 사항을 제공**하는 서비스입니다. 수십만 명의 AWS 고객에게 서비스를 제공하면서 배운 모범 사례를 기반으로 합니다. 지원 계획에 따라 Trusted Advisor 콘솔 또는 AWS Support API를 통해 다양한 검사에 액세스할 수 있습니다. 또한 **Amazon CloudWatch 이벤트를 사용하여 Trusted Advisor 검사의 상태를 모니터링**할 수 있습니다. Trusted Advisor는 AWS Management Console에서 액세스할 수 있으며 이에 대한 액세스를 관리할 수 있습니다.



비용 최적화 (Cost Optimization)
잠재적으로 비용을 절감할 수 있는 권장 사항. 이러한 검사는 사용되지 않는 리소스와 청구서를 줄일 수 있는 기회를 강조합니다.

성능(Performance)
애플리케이션의 속도와 응답성을 개선할 수 있는 권장 사항입니다.

보안(Security)
AWS 솔루션의 보안을 강화할 수 있는 보안 설정에 대한 권장 사항입니다.

내결함성(Fault Tolerance)
AWS 솔루션의 복원력을 높이는 데 도움이 되는 권장 사항입니다.
이러한 검사는 중복 부족, 현재 서비스 제한(할당량이라고도 함) 및 과다 사용된 리소스를 강조합니다.

서비스 제한(Service Limits)
계정에 대한 사용량과 계정이 AWS 서비스 및 리소스에 대한 제한(할당량이라고도 함)에 근접하거나 초과하는지 여부를 확인합니다.

AWS Trusted Advisor

사용

- 사용되지 않거나 활용도가 낮은 리소스를 식별하여 비용 절감 가능
- 보안 취약점 및 잠재적인 규정 준수 문제 파악
- 애플리케이션의 성능 및 응답성 향상
- 중복성 부족 및 과도하게 사용된 리소스를 파악하여 복원력 향상
- 계정의 사용량이 AWS 서비스 및 리소스의 제한(할당량)에 근접하거나 초과하는지 확인

예제

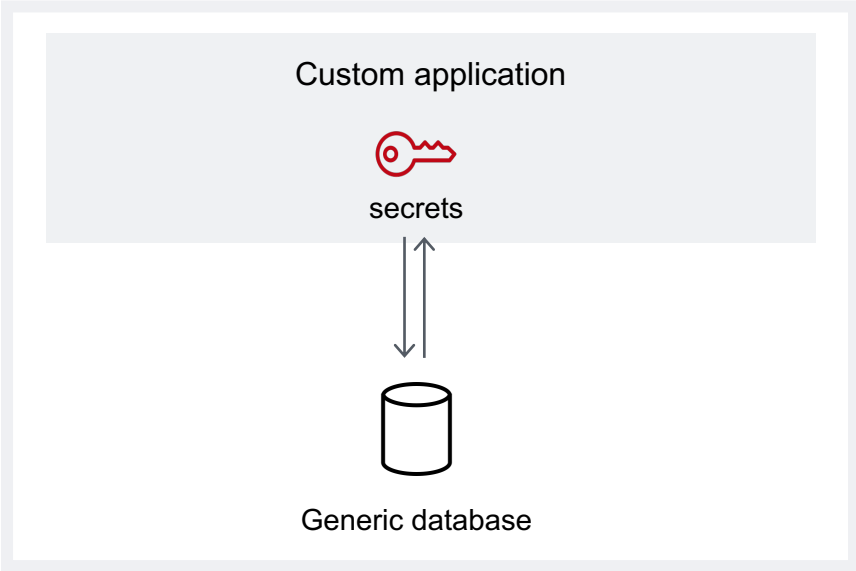
- 월간 AWS 요금을 줄이고자 합니다.중지된 EC2(Amazon Elastic Compute Cloud) 인스턴스와 같은 사용되지 않는 리소스를 식별하고 삭제하여 비용을 절감합니다.
- AWS 환경의 보안을 개선하려고 합니다. Amazon EC2(Elastic Compute Cloud) 인스턴스의 열린 포트와 같은 보안 취약성을 식별하고 이를 완화하기 위한 단계를 수행합니다.
- 응용 프로그램의 성능을 개선하려고 합니다. EBS(Amazon Elastic Block Store) 볼륨 및 ELB(Amazon Elastic Load Balancing) 구성과 관련된 문제를 식별하고 성능을 개선하기 위한 단계를 수행합니다.
- AWS 환경의 복원력을 높이고자 합니다. IOPS 제한에 근접한 Amazon EBS(Elastic Block Store) 볼륨과 같은 중복 부족 및 과도하게 사용되는 리소스를 식별하고 복원력을 높이기 위한 단계를 수행합니다.
- AWS 사용량을 모니터링하려고 합니다. 계정 사용이 AWS 서비스 및 리소스의 제한(할당량)에 근접하거나 초과하는지 확인합니다.

Trusted Advisor는 **권장 사항을 제공하는 서비스**이지 식별되는 문제를 자동으로 해결하는 서비스가 아니라는 점에 유의해야 합니다. **권장 사항을 준수하고 문제를 해결하기 위한 조치를 취할 것인지 여부는 사용자**에게 달려 있습니다.

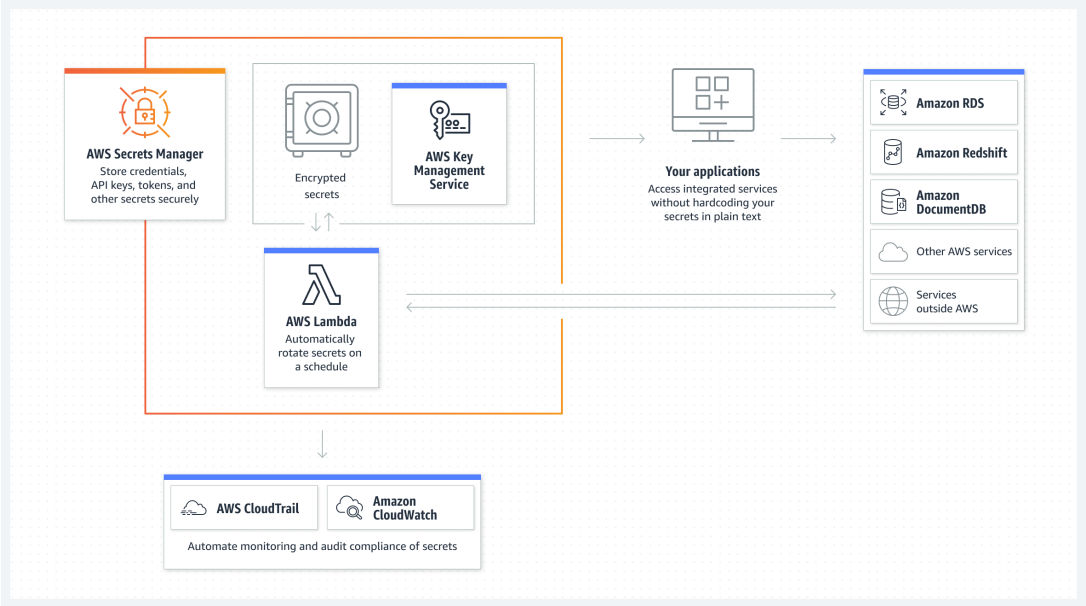
AWS
Secrets Manager

AWS Secrets Manager

AWS 보안, 자격 증명 및 규정 준수 서비스 중, **보안 암호의 수명 주기를 중앙에서 관리하는 데이터 보호 서비스**입니다. 과거에는 응용프로그램에 인증 정보를 포함하는 방식이 일반적이었습니다. 이 방식은 자격 증명 교체 시 많은 작업을 거쳐야 하는 등의 단점이 있습니다.
Secrets Manager 사용 시, **하드 코딩된 자격 증명을 Secrets Manager에 대한 API 호출로 대체하며, 지정된 예약에 따라 자동으로 암호가 순환**되도록 구성할 수 있습니다.



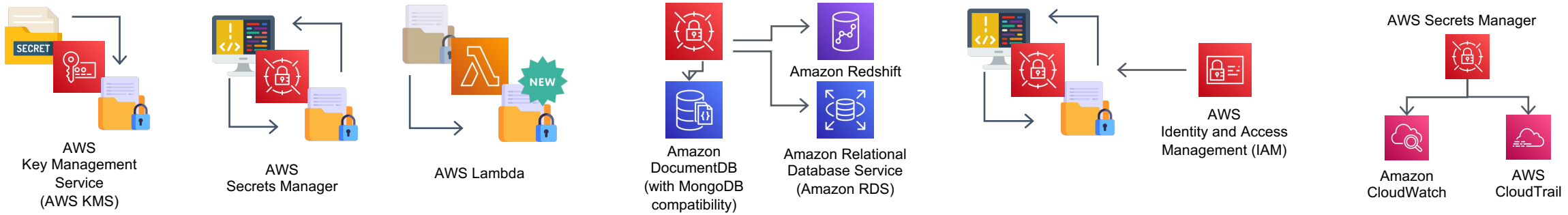
자격증명 교체 시 많은 작업을 거쳐야 하는 단점
새 자격 증명 생성, 응용 프로그램 업데이트,
업데이트된 응용프로그램 재 배포
시간 비용 및 보안 문제



하드코딩된 자격 **증명을 Secrets Manager에 대한 API 호출**로 대체
지정된 예약에 따라 **자동으로 암호 순환 구성** 가능

AWS Secrets Manager

Secrets Manager의 특징과 함께 사용되는 서비스



1. AWS KMS로 자격 증명 데이터 암호화
모든 암호를 KMS 키와 연결하여 자격 증명 암호화, TLS 등을 사용하는 안전한 호스트의 요청만 받아들여 전송 계층 보안 강화

2. 프로그래밍 방식으로 자격증명 동적 검색
런타임에 프로그래밍 방식으로 암호화된 자격 증명 동적 검색 및 보안 상태 개선

3. Lambda를 통한 자동 자격증명 순환
사용자 개입 없이 지정된 일정에 따라 자동으로 암호 순환 가능 및 AWS Lambda 함수를 사용하여 순환 기준 정의

4. 모든 구성이 완료된 서비스 즉시 함께 사용 가능
Amazon Aurora on Amazon RDS 등 모든 암호 순환 구성이 완료되어 있는 데이터베이스 및 서비스 즉시 사용 가능

5. IAM을 통한 자격증명 관리 제한 설정
AWS IAM 권한 정책을 사용하여 Secret Manager 및 암호에 대한 관리 제한 가능
다양한 암호들 중 특정 암호만 읽을 수 있도록 하는 권한 또한 설정 가능

Others

Others

AWS Control Tower 고객이 모범 사례를 기반으로 안전한 다중 계정 AWS 환경을 설정하고 관리할 수 있도록 지원하는 서비스

AWS Organizations 고객이 여러 AWS 계정을 하나의 통합된 엔티티로 생성하고 관리할 수 있는 서비스

AWS Well-Architected Tool 고객이 아키텍처를 검토하고 개선 기회를 식별할 수 있도록 지원하는 서비스

AWS Budgets 고객이 AWS 비용에 대한 예산과 경고를 설정할 수 있는 서비스

AWS License Manager 고객이 클라우드에서 소프트웨어 라이센스를 관리할 수 있는 서비스

AWS Service Catalog 고객이 IT 서비스를 생성, 관리 및 배포할 수 있는 서비스

AWS OpsWorks 고객이 Chef와 Puppet을 사용하여 애플리케이션과 인프라를 관리할 수 있는 서비스

Others

AWS Marketplace	고객이 클라우드에서 소프트웨어를 찾고 구매하고 배포할 수 있는 서비스
Amazon CloudWatch	고객이 리소스와 애플리케이션을 모니터링할 수 있는 서비스
Amazon Managed Grafana	고객이 대시보드를 쉽게 만들고 공유하여 여러 소스의 데이터를 시각화할 수 있는 서비스
Amazon Managed Service for Prometheus	고객이 애플리케이션에서 메트릭 및 경고를 쉽게 수집하고 저장할 수 있는 서비스
AWS CloudTrail	고객이 리소스의 변경 사항을 추적하고 문제를 해결할 수 있는 서비스
AWS Cost Report	고객에게 자세한 비용 및 사용량 보고서를 제공하는 서비스
AWS Cost Explorer	고객이 시간 경과에 따른 비용 및 사용량을 분석할 수 있는 서비스

Others

AWS Managed Services	고객에게 AWS 리소스에 대한 사전 예방적 관리 및 지원을 제공하는 서비스
AWS Service Management Connector	고객이 기존 ITSM(IT Service Management) 툴 내에서 AWS 리소스를 관리할 수 있는 서비스
AWS X-Ray	고객이 애플리케이션 문제를 해결하고 최적화할 수 있는 서비스
AWS Distro for OpenTelemetry	고객이 애플리케이션에서 메트릭, 추적 및 로그를 수집하고 내보낼 수 있는 서비스
AWS Proton	고객이 컨테이너형 애플리케이션을 선언적으로 배포하고 관리할 수 있는 서비스
Amazon DevOps Guru	운영상의 문제를 자동으로 감지하고 성능 향상을 위한 조치를 추천하는 서비스

Thanks!