



애플리케이션 소유자를 위한 로깅 및 모니터링 가이드

# AWS 규범적 지침



# AWS 규범적 지침: 애플리케이션 소유자를 위한 로깅 및 모니터링 가이드

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

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

# Table of Contents

소개 .....	1
목표 비즈니스 성과 .....	1
애플리케이션의 로깅 및 모니터링 정보 .....	2
애플리케이션 로깅 .....	3
이벤트 유형 .....	3
이벤트 속성 .....	4
모범 사례 .....	9
로깅 수준 .....	9
주의 및 제외 .....	9
특수 데이터 유형 .....	10
액세스 및 변경 관리 .....	10
로깅 및 모니터링을 위한 AWS 서비스 .....	12
CloudTrail .....	13
CloudTrail 사용 .....	13
CloudTrail의 사용 사례 .....	13
CloudTrail 모범 사례 .....	14
CloudWatch .....	15
CloudWatch 사용 .....	15
CloudWatch의 사용 사례 .....	15
CloudWatch Logs .....	16
CloudWatch Logs 사용 .....	16
CloudWatch Logs의 사용 사례 .....	17
VPC 흐름 로그 .....	17
VPC Flow Logs 사용 .....	18
VPC Flow Logs 사용 사례 .....	18
X-Ray .....	19
X-Ray 사용 .....	19
Xray의 사용 사례 .....	19
FAQ .....	20
현재 사용 중인 모니터링 서비스를 사용할 수 있나요? .....	20
로그 파일이 변조되지 않도록 하려면 어떻게 해야 하나요? .....	20
각 애플리케이션마다 별도의 로그 파일을 유지해야 하나요? .....	20
리소스 .....	21
AWS 설명서 .....	21

---

AWS 마케팅 .....	21
문서 기록 .....	22
용어집 .....	23
# .....	23
A .....	24
B .....	26
C .....	28
D .....	30
E .....	34
F .....	36
G .....	37
H .....	38
I .....	39
L .....	41
M .....	42
O .....	45
P .....	47
Q .....	49
R .....	49
S .....	52
T .....	55
U .....	56
V .....	57
W .....	57
Z .....	58
.....	lix

# 애플리케이션 소유자를 위한 로깅 및 모니터링 가이드

John Buckley, Amazon Web Services(AWS)

2023년 1월([문서 기록](#))

워크로드란 고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음을 말합니다. 워크로드는 단일 AWS 계정의 리소스 하위 세트로 구성되거나 여러 AWS 계정에 걸쳐 있을 수 있습니다. 클라우드에서 애플리케이션은 워크로드의 한 유형입니다. 애플리케이션은 클라우드 환경에만 배포되거나 로컬 온프레미스 하드웨어에서 지원될 수도 있습니다. 많은 출판물이 클라우드 인프라 로깅 및 모니터링에 중점을 두고 있으며 보안 팀을 대상으로 합니다. 이 가이드는 애플리케이션 소유자를 대상으로 하며 AWS 클라우드에서 애플리케이션을 로깅하고 모니터링하기 위한 효과적이고 효율적인 접근 방식에 중점을 둡니다.

이 가이드는 이상 징후를 신속하게 식별하고 이에 대응할 수 있도록 적절한 수준의 로깅과 모니터링을 설정하는 데 도움이 됩니다. 또한 애플리케이션 로그가 모든 문제에 대한 자세한 분석 및 해결을 지원 하는지 확인하는 데도 도움이 됩니다.

이 가이드는 AWS 클라우드 배포를 염두에 두고 작성되었지만 이러한 원칙을 온프레미스 또는 다른 클라우드 제공업체 인프라에서 실행되는 애플리케이션에 적용할 수 있습니다.

## 목표 비즈니스 성과

이 가이드를 읽고 나면 다음 사항을 이해할 수 있습니다.

- 애플리케이션에 대해 일반적으로 기록되는 이벤트 유형
- 로깅을 고려해야 하는 이벤트 속성(예: 누가, 무엇을, 언제)
- 로그에서 제외하는 것을 고려해야 하는 데이터 유형(예: 보안 태세를 손상시킬 수 있는 데이터 또는 개인 식별 정보)
- 애플리케이션에 적합한 수준의 로깅 및 모니터링을 설정하는 방법
- 애플리케이션 로그를 관리하고 액세스할 수 있는 사용자
- AWS 클라우드에서 애플리케이션을 모니터링하고 기록하도록 구성할 수 있는 AWS 서비스 및 기능
- 애플리케이션과 AWS 서비스 및 기능의 로그 데이터를 사용하여 문제를 분류하고 진단하는 방법

# 애플리케이션의 로깅 및 모니터링 정보

로깅, 모니터링, 알림 및 보고는 애플리케이션의 상태와 성능에 대한 가시성을 제공하기 위해 함께 작동하는 다양한 보안 프로세스입니다. 기록된 활동을 기반으로 모니터링, 알림 및 보고를 수행할 수 있도록 애플리케이션에 대한 자세한 작업 및 이벤트 기록을 만들고 유지 관리하는 것이 중요합니다.

애플리케이션 로깅은 애플리케이션에서 생성된 이벤트를 수집하여 하나 이상의 로그 파일에 기록하는 프로세스입니다. 이 이벤트 기록은 보안 및 성능 분석을 수행하고, 리소스 변경을 추적하고, 애플리케이션 문제를 해결하는 데 도움이 될 수 있습니다.

애플리케이션 모니터링은 애플리케이션의 전반적인 성능과 상태를 평가하는 프로세스입니다. 애플리케이션의 프론트엔드와 백엔드를 지속적으로 모니터링할 수 있어야 합니다. 클라우드에서 호스팅되는 애플리케이션은 고도로 분산되어 있으므로 로깅 및 모니터링 도구를 사용하면 성능 문제를 신속하게 해결하거나 보안 위협을 실시간으로 식별하고 해결할 수 있습니다. 로그 데이터는 모니터링을 위한 중요한 입력입니다.

관찰성은 모니터링과 비슷하지만 다양한 파라미터를 사용하여 애플리케이션 동작을 측정하는 방법도 도입하고 복잡한 상관 관계를 파악할 수 있습니다. 특정 리전의 사용자 집합을 대상으로 특정 날짜의 HTTP 성공률을 측정하는 경우를 예로 들 수 있습니다. 자세한 내용은 [모니터링 및 관측성](#)(AWS 마케팅)을 참조하세요.

궁극적으로 애플리케이션 소유자의 목표는 안전하고 건강한 애플리케이션을 유지하고 해당 애플리케이션에 대한 긍정적인 사용자 경험을 유지하는 것입니다. 로깅 및 모니터링을 구현하면 개발자와 운영 팀이 애플리케이션 문제를 더 빠르게 계획하고 문제를 해결할 수 있습니다.

필요한 로깅 및 모니터링 수준은 애플리케이션마다 다릅니다. 모니터링 및 로깅 수준에 영향을 줄 수 있는 요소에는 조직 정책 및 절차, 애플리케이션이 야기하는 보안 위협 수준, 비즈니스 운영에 대한 애플리케이션의 중요도, 애플리케이션이 관리하는 데이터의 민감도 등이 있습니다. 일반적으로 퍼블릭 또는 고객 대상 애플리케이션은 조직 내부에서 사용되는 애플리케이션보다 높은 수준의 모니터링 및 로깅이 필요합니다. 이 가이드에는 일반적인 정보와 권장 사항이 포함되어 있으므로 애플리케이션의 요구 사항에 따라 접근 방식을 사용자 지정해야 합니다.

## Note

조직의 표준 또는 절차에 따라 특정 로깅 및 모니터링 속성이 필요할 수 있습니다. 사용자 권한을 엔터프라이즈 자격 검토 시스템에 전달하는 경우를 예로 들 수 있습니다. 로깅 및 모니터링 계획이 조직의 요구 사항을 충족하는지 확인합니다.

# AWS 클라우드에서 애플리케이션 로깅

AWS 클라우드의 로깅 애플리케이션에 대해 일반적인 이벤트 유형, 이벤트 속성 및 모범 사례를 검토하세요.

이 섹션에는 다음 주제가 포함되어 있습니다.

- [이벤트 유형](#)
- [이벤트 속성](#)
- [로깅 모범 사례](#)

## 이벤트 유형

애플리케이션 로깅 전략을 수립할 때 가장 중요한 고려 사항 중 하나는 기록할 이벤트와 작업을 결정하는 것입니다. 조직과 애플리케이션의 요구 사항이 이 결정에 영향을 미칠 수 있지만 애플리케이션에 적용되는 경우 항상 다음 사항을 로깅하는 것이 좋습니다.

- 입력 검증 실패 - 프로토콜 위반, 허용되지 않는 인코딩, 잘못된 파라미터 이름 및 값 등을 예로 들 수 있습니다.
- 출력 검증 실패 - 데이터베이스 레코드 세트 불일치 및 잘못된 데이터 인코딩 등을 예로 들 수 있습니다.
- ID 인증 성공 및 실패 - 인증 활동은 로깅하지만 사용자 이름과 암호는 로깅하지 않습니다. 사용자가 실수로 사용자 이름 필드에 암호를 입력할 수 있으므로 사용자 이름은 로깅하지 않는 것이 좋습니다. 이로 인해 의도치 않게 보안 인증 정보가 노출되어 액세스가 승인될 수 있습니다. 인증 데이터가 포함된 모든 로그에 대해 보안 제어를 구현하세요.
- 권한 부여(액세스 제어) 실패 - 관련 권한 부여 시스템에 대해 실패한 액세스 시도를 로깅합니다. 이 로그 데이터를 모니터링하여 애플리케이션의 권한 부여 시스템에 대한 공격 또는 문제를 나타낼 수 있는 패턴이 있는지 확인할 수 있습니다.
- 세션 관리 실패 - 세션 쿠키 또는 토큰 수정을 예로 들 수 있습니다. 애플리케이션은 종종 쿠키나 토큰을 사용하여 사용자 상태를 관리합니다. 악의적인 사용자는 쿠키 값을 수정하여 무단 액세스를 시도할 수 있습니다. 변조된 세션 토큰을 로깅하면 이러한 동작을 탐지할 수 있습니다.
- 애플리케이션 오류 및 시스템 이벤트 - 구문 및 런타임 오류, 연결 문제, 성능 문제, 타사 서비스의 오류 메시지, 파일 시스템 오류, 파일 업로드를 위한 바이러스 탐지, 구성 변경 등을 예로 들 수 있습니다.
- 애플리케이션 상태 - 애플리케이션과 관련 리소스를 시작하거나 중지하고 있습니다.

- 로깅 상태 - 로깅을 시작, 중지 또는 일시 중지하고 있습니다.
- 위험도가 높은 기능 사용 - 네트워크 연결 변경, 사용자 추가 또는 삭제, 권한 변경, 토큰에 사용자 할당, 토큰 추가 또는 삭제, 시스템 관리 권한 사용, 애플리케이션 관리자의 액세스, 관리자 권한이 있는 사용자가 수행하는 모든 작업, 결제 카드 소유자 데이터 액세스, 데이터 암호화 키 사용, 암호화 키 변경, 시스템 수준 객체 생성 및 삭제, 사용자 생성 콘텐츠 제출(특히 파일 업로드), 데이터 가져오기 및 내보내기(보고서 포함) 등을 예로 들 수 있습니다.
- 법률 및 기타 옵트인 - 휴대폰 기능에 대한 권한, 이용 약관, 약관, 개인 데이터 사용 동의, 마케팅 커뮤니케이션 수신 권한 등을 예로 들 수 있습니다.

애플리케이션에 대한 권장 속성 외에도 모니터링, 알림 및 보고에 유용한 데이터를 제공할 수 있는 추가 속성은 무엇인지 생각해 보세요. 예:

- 시퀀싱 실패
- 조직의 허용 가능한 사용 정책을 위반하는 사용자 행동을 평가하는 데 도움이 되는 속성
- 데이터 변경
- 표준 또는 규정을 준수하는 데 필요한 속성(예: 금융 범죄 예방, 주식 거래 제한, 건강 또는 기타 개인 정보 수집)
- 무단 조치 시도 등 의심스럽거나 예상치 못한 행동을 식별하는 데 도움이 되는 속성
- 구성 변경
- 애플리케이션 코드 파일 또는 메모리 변경

## 이벤트 속성

각 로그 항목에는 모니터링 및 분석을 위한 충분히 세부 정보가 포함되어야 합니다. 전체 콘텐츠 데이터를 로깅할 수도 있지만 추출 또는 요약 속성을 기록하는 것이 더 효율적입니다. 애플리케이션 로그에는 각 이벤트의 언제, 어디서, 누가, 무엇, 어떤 속성을 기록해야 합니다. 이들 속성은 아키텍처, 애플리케이션 클래스, 호스트 시스템 또는 디바이스에 따라 달라집니다.

날짜 및 시간 스탬프를 기록할 때 협정 세계시(UTC)와 [ISO 8601](#)(ISO 웹 사이트)에서 국제적으로 인정되는 날짜 및 시간 형식을 사용하세요.

### Note

타임스탬프가 정확한지 확인하려면 네트워크 시간 동기화 서비스를 사용하는 것이 좋습니다. Amazon은 Amazon Elastic Compute Cloud(Amazon EC2)를 비롯한 많은 AWS 서비스에서 사



용되는 Amazon Time Sync Service를 제공합니다. Amazon Time Sync Service에서는 각 AWS 리전의 위성 연결 및 원자 기준 시계의 풀릿을 사용하여 NTP(Network Time Protocol)를 통해 UTC 세계 표준의 정확한 현재 시간 판독값을 제공합니다. 자세한 내용은 [Keeping Time with Amazon Time Sync Service](#)(AWS 블로그 게시물)를 참조하세요.

로그에는 일반적으로 다음과 같은 이벤트 속성이 포함됩니다.

속성 범주	이벤트 속성	설명
일시	로깅 날짜 및 시간	이벤트가 로그에 추가된 날짜와 시간을 기록합니다.
	현재 날짜 및 시간	이벤트가 발생한 날짜와 시간을 기록합니다. 이는 클라이언트 애플리케이션이 정기적으로 또는 간헐적으로 온라인 상태인 원격 디바이스에서 호스팅되기 때문에 로깅이 지연되는 경우와 같이 로깅 레코드와 다를 수 있습니다.
어디서	이벤트 식별자	이벤트를 항상 식별할 수 있도록 사용자 이름, 계정 번호 또는 기타 고유한 속성을 기록하세요.
	애플리케이션 식별자	애플리케이션 이름과 버전을 로깅합니다.
	애플리케이션 주소	클러스터 또는 호스트 이름, 서버 IPv4 또는 IPv6 주소, 포트 번호, 워크스테이션 ID, 로컬 디바이스 식별자를 로깅합니다.
	서비스	서비스 이름과 프로토콜을 로깅합니다.

	지리적 위치	사용자의 지리적 위치를 로깅합니다.
	창, 양식 또는 페이지	진입점 URL, 웹 애플리케이션의 HTTP 메서드 또는 작업이 수행된 대화 상자 이름을 로깅합니다.
	코드 위치	스크립트 또는 모듈 이름을 로깅합니다.
누가(인간 또는 컴퓨터 사용자)	소스 주소	사용자의 디바이스 식별자, IP 주소, 셀룰러 또는 무선 주파수 (RF) 타워 ID 또는 휴대폰 번호를 로깅합니다.
	사용자 자격 증명	사용자가 인증되었거나 알려진 경우 사용자 데이터베이스 테이블의 프라이머리 키 값, 사용자 이름 또는 라이선스 번호를 로깅합니다.
	사용자 유형 분류	퍼블릭, 인증, CMS, 검색 엔진, 공인 침투 테스터 또는 가동 시간 모니터와 같은 사용자 유형을 로깅합니다. 가동 시간 모니터에 대한 자세한 내용은 이 가이드의 <a href="#">주의 및 제외</a> 섹션을 참조하세요.
	HTTP 헤더 또는 HTTP 사용자 에이전트 요청	(웹 애플리케이션만 해당) HTTP 사용자 에이전트 문자열을 비롯한 HTTP 요청 헤더 정보를 로깅합니다. 이러한 값은 클라이언트가 서버로 보내는 정보에 영향을 미치기 때문입니다.

무엇	이벤트 유형	이벤트가 정보용인지, 알림인지, 오류인지를 로깅합니다.
	이벤트 심각도	이벤트 심각도를 높음, 중간, 낮음 등으로 분류합니다.
	보안 이벤트 플래그	로그에 보안 이벤트와 관련 없는 데이터가 포함되어 있는 경우 보안 관련 이벤트에 대한 플래그를 생성하여 식별할 수 있도록 합니다.
	이벤트 설명	(선택 사항) 이벤트에 대한 간략한 설명을 포함합니다.
	행동 또는 의도	로그인, 세션 ID 새로 고침, 로그아웃, 프로파일 업데이트 등 요청의 원래 의도된 목적을 기록합니다.
	사용자 또는 애플리케이션 응답	이벤트에 대한 사용자 또는 애플리케이션의 응답(예: 상태 코드, 사용자 지정 문자 메시지, 세션 중지 또는 관리자 알림)을 로깅합니다.
	결과 상태	작업의 성공 여부(예: 성공, 실패 또는 연기)를 로깅합니다.
	결과 이유	상태가 발생한 이유를 로깅합니다. 예를 들어, 사용자가 데이터베이스에서 인증되지 않아 로그인 요청이 실패할 수 있습니다.

	확장된 세부 정보	스택 추적, 시스템 오류 메시지, 디버그 정보, HTTP 요청 본문 등 이벤트와 관련된 추가 정보를 모두 로깅합니다.
	HTTP 응답 상태 코드	(웹 애플리케이션만 해당) 사용자에게 반환된 HTTP 응답 상태 코드(예: 200 또는 301)를 로깅합니다. 자세한 내용은 이 가이드의 <a href="#">로깅 수준</a> 을 참조하세요.
어떤	영향을 받는 리소스	어떤 리소스가 사용되었는지 로깅합니다.
	객체	영향을 받는 구성 요소나 기타 객체(예: 사용자 계정, 데이터 리소스, 파일, URL 또는 세션 ID)를 로깅합니다.
	리소스 이름	영향을 받는 리소스의 이름을 로깅합니다.
	리소스 태그	영향을 받는 리소스에 할당된 태그를 로깅합니다. 태그에 대한 자세한 내용은 <a href="#">AWS 리소스 태깅</a> (AWS 일반 참조 안내서)을 참조하세요.
기타	분석 신뢰도	이벤트 감지에 대한 로깅 서비스의 신뢰도를 기록합니다(예: 낮음, 중간 또는 높은 등급 지정 또는 숫자 값 지정).
	내부 분류	표준 또는 규정 준수를 위해 모든 내부 분류를 로깅합니다.

## 내부 분류

표준 또는 규정 준수를 위한 모든 외부 분류(예: NIST SCAP(Security Content Automation Protocol))를 로깅합니다.

# 로깅 모범 사례

## 로깅 수준

과도한 양의 데이터를 기록하지 않도록 주의합니다. 로그에는 유용하고 실행 가능한 데이터가 기록되어야 합니다. 과도한 로깅은 성능에 부정적인 영향을 줄 수 있으며 로깅 저장과 처리 비용도 증가할 수 있습니다. 또한 문제와 보안 이벤트가 감지되지 않을 수도 있습니다.

HTTP 응답 상태 코드를 로깅하면 상당한 양의 로그 데이터, 특히 200레벨(성공) 및 300레벨(리디렉션) 상태 코드가 생성될 수 있습니다. 400수준(클라이언트측 오류) 및 500수준(서버측 오류) 상태 코드만 로깅하는 것을 고려하는 것이 좋습니다.

애플리케이션 로깅 프레임워크는 정보, 디버그, 오류 등 다양한 수준의 로깅을 제공합니다. 개발 환경의 경우 개발자를 돕기 위해 정보와 디버그 등의 자세한 로깅을 사용할 수 있습니다. 그러나 과도한 로깅 데이터를 생성할 수 있으므로 프로덕션 환경에서는 정보 및 디버그 수준을 비활성화하는 것이 좋습니다.

## 주의 및 제외

- 로깅하는 데이터가 법적으로 허용되는지 확인하세요(특히 조직이 운영되는 관할 구역에서).
- 알려진 사용자(예: 다른 내부 시스템), 신뢰할 수 있는 타사, 검색 엔진 로봇, 가동 시간 또는 프로세스 모니터, 기타 원격 모니터링 시스템의 이벤트를 제외하지 마세요. 그러나 기록된 데이터에 이들 각 항목에 대한 분류 플래그를 포함할 수 있습니다. 애플리케이션에서 생성되는 로그 파일은 애플리케이션에서 처리하는 민감한 데이터를 볼 권한이 없는 타사 로그 모니터링 솔루션 또는 외부 서비스 제공업체 등에서 사용할 수 있다는 점을 고려하세요.
- 다음 속성은 로그에 직접 기록되어서는 안 됩니다. 다음 항목을 제거, 마스킹, 삭제, 해시 또는 암호화하세요.
  - 애플리케이션 소스 코드
  - 세션 식별 값(세션별 이벤트를 추적해야 하는 경우 해시된 값으로 바꾸는 것이 좋음)
  - 액세스 토큰

- 민감한 개인 데이터 및 일부 형태의 개인 식별 정보(PII)(예: 건강 정보 또는 정부가 발행한 신분증)
- 인증 암호
- 데이터베이스 연결 문자열
- 암호화 키 및 기타 기본 시크릿
- 은행 계좌 또는 결제 카드 소유자 데이터
- 로깅 시스템이 저장할 수 있는 보다 높은 보안 등급의 데이터
- 상업적으로 민감한 정보
- 해당 관할 구역에서 수집이 불법인 정보
- 사용자가 수집을 거부했거나 수집에 명시적으로 동의하지 않은 정보
- 수집 동의가 만료된 정보

## 특수 데이터 유형

경우에 따라 다음과 같은 데이터가 로그에 기록될 수도 있습니다. 조사 및 문제 해결 목적으로 유용할 수 있지만 시스템에 대한 민감한 정보가 노출될 수 있습니다. 이벤트가 기록되기 전에 다음과 같은 데이터 유형을 익명화, 해시 또는 암호화해야 할 수 있습니다.

- 파일 경로
- 내부 네트워크 이름 및 주소
- 개인 이름, 전화번호, 이메일 주소 등 민감하지 않은 개인 데이터

로그에 개인의 실제 신원이 필요하지 않거나 너무 위험하다고 간주되는 경우 데이터 익명화를 사용하세요.

## 액세스 및 변경 관리

- 관리자가 아닌 사용자는 특히 규정 준수 요구 사항을 충족하는 데 필요한 이벤트 로깅을 비활성화할 수 없어야 합니다.
- 관리자만 로깅 서비스를 일시 중지 또는 중지하거나 구성을 수정할 수 있어야 합니다.
- 로깅 서비스에 로그 파일 무결성 검증 기능이 있는 경우 해당 기능을 활성화하세요. 이렇게 하면 로그 파일의 수정, 삭제 또는 위조를 감지하는 데 도움이 됩니다. AWS 서비스의 이 기능에 대한 자세한 내용은 이 가이드의 [CloudTrail 사용](#) 섹션을 참조하세요.

- 변경 사항 로깅은 승인된 알고리즘을 기반으로 애플리케이션에 의해 자동으로 수행되는 것과 같이 애플리케이션에 내장된 것이거나 구성 데이터를 변경하거나 소스 코드를 수정하는 경우와 같이 승인된 변경 관리 프로세스를 따라야 합니다.

## 로깅 및 모니터링을 위한 AWS 서비스

이 가이드는 AWS 클라우드에 배포된 애플리케이션을 로깅하고 모니터링하는 데 중점을 둡니다. AWS 서비스를 사용하여 로깅 및 모니터링 계획을 구현하거나 현재 솔루션을 강화할 수 있습니다. 예를 들어, 애플리케이션 문제를 해결하는 경우 다음과 같은 조치를 취할 수 있습니다.

- Amazon Virtual Private Cloud(Amazon VPC)의 VPC Flow Logs 기능을 사용하여 애플리케이션 로그를 분류하고 문제에 해당하는 네트워크 트래픽을 확인합니다.
- AWS CloudTrail을 사용하여 문제 이벤트 시간에 해당하는 API 호출을 봅니다.
- Amazon CloudWatch Logs의 로그를 검토하여 문제 이벤트 시간에 해당하는 CPU 스파이크가 있는지 검토합니다.

애플리케이션 로깅 및 모니터링을 위해 다음 AWS 서비스 및 기능을 배포할 수 있습니다.

- [AWS CloudTrail](#)은 사용자, 역할 또는 AWS 서비스이 수행한 작업을 기록하여 AWS 계정의 거버넌스, 규정 준수 및 운영 위험을 감사하는 데 도움이 됩니다. 이 서비스를 사용하여 애플리케이션의 이벤트를 로깅하거나 모니터링하는 방법에 대한 자세한 내용은 이 가이드의 [CloudTrail](#) 섹션을 참조하세요.
- [Amazon CloudWatch](#)를 사용하면 AWS 리소스 및 호스팅된 애플리케이션의 로그를 분석하고 측정치를 실시간으로 모니터링할 수 있습니다. 또한 ServiceLens 기능을 사용하여 애플리케이션의 상태를 모니터링하거나 Synthetics 기능을 사용하여 엔드포인트와 API를 모니터링하는 canary를 생성할 수 있습니다. 이 서비스를 사용하여 애플리케이션을 모니터링하는 방법에 대한 자세한 내용은 이 가이드의 [CloudWatch](#) 섹션을 참조하세요.
- [Amazon CloudWatch Logs](#)는 모든 시스템, 애플리케이션 및 AWS 서비스의 로그를 중앙 집중화하여 모니터링하고 안전하게 보관할 수 있도록 도와줍니다. 이 서비스를 사용하여 애플리케이션의 이벤트를 로깅하는 방법에 대한 자세한 내용은 이 가이드의 [CloudWatch Logs](#) 섹션을 참조하세요.
- Amazon Virtual Private Cloud(VPC)의 [VPC 흐름 로그](#) 기능은 VPC의 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처합니다. 이 서비스를 사용하여 애플리케이션의 이벤트를 로깅하는 방법에 대한 자세한 내용은 이 가이드의 [VPC 흐름 로그](#) 섹션을 참조하세요.
- [AWS X-Ray](#)는 애플리케이션이 처리하는 요청에 대한 데이터를 수집하며, 해당 데이터를 보고, 필터링하고, 인사이트를 얻어 최적화에 대한 문제와 기회를 파악하는 데 도움이 됩니다. 이 서비스를 사용하여 애플리케이션을 모니터링하는 방법에 대한 자세한 내용은 이 가이드의 [X-Ray](#) 섹션을 참조하세요.



# AWS CloudTrail를 사용하여 애플리케이션 로깅 및 모니터링

[AWS CloudTrail](#)은 AWS 계정에 대한 운영 및 위험 감사, 거버넌스 및 규정 준수를 활성화하는 데 도움이 되는 AWS 서비스 서비스입니다. 사용자, 역할 또는 AWS 서비스) 수행하는 작업은 CloudTrail에 이벤트로 기록됩니다. 이벤트에 AWS Management Console, AWS Command Line Interface(AWS CLI) 및 AWS SDK와 API에서 수행되는 작업이 포함될 수 있습니다.

## CloudTrail 사용

CloudTrail은 AWS 계정을 생성할 때 활성화됩니다. 활동이 AWS 계정에서 이루어지면 해당 활동이 CloudTrail 이벤트에 기록됩니다. 이벤트 기록으로 이동해서 CloudTrail 콘솔에서 손쉽게 최신 이벤트를 확인할 수 있습니다.

AWS 계정의 지속적인 활동 및 사건 기록을 위해 트레일을 생성합니다. 단일 AWS 리전 또는 모든 리전에 대한 트레일을 생성할 수 있습니다. 트레일은 각 리전의 로그 파일을 기록하고 CloudTrail은 로그 파일을 단일 통합 Amazon Simple Storage Service(S3) 버킷으로 전송할 수 있습니다.

추적이 지정한 이벤트만 처리하고 로깅하도록 여러 추적을 다르게 구성할 수 있습니다. 이는 AWS 계정에서 발생하는 이벤트를 애플리케이션에서 발생하는 이벤트와 함께 분류하려는 경우 유용할 수 있습니다.

### Note

CloudTrail에는 CloudTrail이 로그 파일을 전송한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인하는 데 사용할 수 있는 검증 기능이 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다. AWS CLI를 사용하면 CloudTrail이 로그 파일을 전송한 위치에서 파일을 검증할 수 있습니다. 이 기능 및 사용 방법에 대한 자세한 내용은 [Validating CloudTrail log file integrity](#)(CloudTrail 설명서)를 참조하세요.

## CloudTrail의 사용 사례

- 규정 준수 지원 - CloudTrail을 사용하면 AWS 계정의 이벤트 기록을 제공하여 내부 정책 및 규제 표준을 준수하는 데 도움이 될 수 있습니다.

- 보안 분석 - CloudTrail 로그 파일을 CloudWatch Logs, Amazon EventBridge, Amazon Athena, Amazon OpenSearch Service 또는 기타 타사 솔루션과 같은 로그 관리 및 분석 솔루션에 수집하여 보안 분석을 수행하고 사용자 행동 패턴을 탐지할 수 있습니다.
- 데이터 유출 - CloudTrail에 기록된 객체 수준 API 이벤트를 통해 Amazon S3 객체의 활동 데이터를 수집하여 데이터 유출을 탐지할 수 있습니다. 활동 데이터가 수집된 후 EventBridge, AWS Lambda 등의 다른 AWS 서비스를 사용하여 자동 응답을 트리거할 수 있습니다.
- 운영 문제 해결 - CloudTrail 로그 파일을 사용하여 운영 문제를 해결할 수 있습니다. 예를 들어, AWS 리소스 생성, 수정, 삭제를 포함하여 환경 내 리소스에 대한 가장 최근의 변경 사항을 빠르게 식별할 수 있습니다.

## CloudTrail 모범 사례

- 모든 AWS 리전에서 CloudTrail을 활성화합니다.
- 로그 파일 무결성 검증을 활성화합니다.
- 로그를 암호화합니다.
- CloudTrail 로그 파일을 CloudWatch Logs에 모읍니다.
- 모든 AWS 계정과 리전의 로그를 중앙 집중화합니다.
- 수명 주기 정책을 로그 파일이 포함된 S3 버킷에 적용합니다.
- 사용자가 CloudTrail에서 로깅을 끌 수 없도록 합니다. AWS Organizations에서 다음 [서비스 제어 정책\(SCP\)](#)을 적용합니다. 이 SCP는 조직 전체의 StopLogging 및 DeleteTrail 작업에 대한 명시적인 거부 규칙을 설정합니다.

```
{
  "Version": "2012-10-17",
  "Statement":
    [
      { "Action":
        [
          "cloudtrail:StopLogging",
          "cloudtrail>DeleteTrail"
        ],
        "Resource": "*",
        "Effect": "Deny"
      }
    ]
}
```

# Amazon CloudWatch를 사용한 애플리케이션 로깅 및 모니터링

[Amazon CloudWatch](#)는 AWS에서 실행하는 AWS 리소스와 애플리케이션을 실시간으로 모니터링합니다. CloudWatch를 사용하여 리소스 및 애플리케이션에 대해 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다.

## CloudWatch 사용

CloudWatch는 기본적으로 지표 리포지토리입니다. Amazon EC2와 같은 AWS 서비스는 지표를 리포지토리에 저장하므로 이러한 지표를 기반으로 통계를 검색할 수 있습니다. 사용자 지정 지표를 리포지토리에 저장하면 이러한 지표에 대한 통계도 검색할 수 있습니다. 자세한 내용은 [CloudWatch 지표 사용](#)(CloudWatch 설명서)을 참조하세요.

사용자를 대신하여 자동으로 작업을 시작하는 경보를 구성할 수도 있습니다. 경보는 지정한 기간에 단일 지표를 감시하고 시간에 따른 임계값에 대한 지표 값을 기준으로 지정된 작업을 하나 이상 수행합니다. 예를 들어, 경보는 Amazon Simple Notification Service(SNS) 주제에 알림을 보낼 수 있습니다. 대시보드에 경보를 추가할 수도 있습니다. 자세한 내용은 [CloudWatch 경보 사용](#)(CloudWatch 설명서)을 참조하세요.

CloudWatch 콘솔에는 사용 중인 모든 AWS 서비스에 대한 지표가 자동으로 표시됩니다. 애플리케이션에 대한 지표와 경보를 표시하는 추가 사용자 지정 대시보드를 만들 수 있습니다. 자세한 내용은 [CloudWatch 대시보드 사용](#)(CloudWatch 설명서)을 참조하세요.

CloudWatch는 크로스 리전 기능을 자동으로 지원합니다. 동일한 그래프나 대시보드에서 단일 계정으로 여러 AWS 리전의 지표를 표시하기 위해 추가 단계를 수행할 필요가 없습니다. [크로스 계정 관찰성](#)을 구현하여 크로스 계정 기능을 달성할 수 있습니다(CloudWatch 설명서).

AWS 클라우드에서 CloudWatch를 사용하여 워크로드를 기록하고 모니터링하는 방법에 대한 자세한 내용과 지침은 [Designing and implementing logging and monitoring with Amazon CloudWatch](#)(AWS 권장 가이드)를 참조하세요.

## CloudWatch의 사용 사례

- 애플리케이션 상태 모니터링 - CloudWatch ServiceLens를 사용하면 추적, 지표, 로그, 경보 및 기타 리소스 상태 정보를 한 곳에 통합할 수 있으므로 서비스 및 애플리케이션의 관찰성이 향상됩니다. ServiceLens는 CloudWatch를 AWS X-Ray와 통합하여 애플리케이션에 대한 전체적인 보기를 제공함으로써 성능 병목 현상을 더욱 효율적으로 파악하고 영향을 받는 사용자를 식별하도록 지원합니다. 자세한 내용은 [ServiceLens를 사용하여 애플리케이션의 상태 모니터링](#)(CloudWatch 설명서)을 참조하세요.

- **Synthetics 모니터링** – Amazon CloudWatch Synthetics를 사용하여 일정에 따라 실행되는 구성 가능한 스크립트인 canary를 생성하여 엔드포인트 및 API를 모니터링할 수 있습니다. canary는 동일한 경로를 따라 고객과 동일한 작업을 수행하므로 애플리케이션에 고객 트래픽이 없는 경우에도 고객 경험을 지속적으로 확인할 수 있습니다. canary는 엔드포인트의 가용성과 지연 시간을 확인하고 로드 시간 데이터 및 UI 스크린샷을 저장할 수 있습니다. REST API, URL 및 웹사이트 콘텐츠를 모니터링하고 피싱, 코드 주입 및 교차 사이트 스크립팅으로 인한 무단 변경 사항을 검사할 수 있습니다. 자세한 내용은 [Synthetics 모니터링 사용](#)(CloudWatch 설명서)을 참조하세요.
- **사용자 모니터링** – CloudWatch RUM을 사용하면 실제 사용자 모니터링을 수행하여 웹 애플리케이션 성능에 대한 클라이언트측 데이터를 수집하고 볼 수 있습니다. 데이터에는 페이지 로드 시간, 클라이언트측 오류 및 사용자 동작이 포함됩니다. 수집된 데이터를 사용하여 클라이언트측 성능 문제를 신속하게 식별하고 디버깅할 수 있습니다. 자세한 내용은 [CloudWatch RUM 사용](#)(CloudWatch 설명서)을 참조하세요.
- **이상 동작 탐지** – 지표에 대해 이상 탐지를 활성화하면 CloudWatch는 통계 및 기계 학습 알고리즘을 적용합니다. 이러한 알고리즘은 시스템 및 애플리케이션의 지표를 지속적으로 분석하고, 정상 기준을 결정하고, 이상 징후를 표면화합니다. 자세한 내용은 [CloudWatch 이상 탐지 사용](#)(CloudWatch 설명서)을 참조하세요.
- **기능 검증 및 A/B 실험** – Amazon CloudWatch Evidently를 사용하면 기능을 롤아웃하는 중에 지정된 비율의 사용자에게 제공하여 새 기능을 안전하게 검증할 수 있습니다. 또한 A/B 실험을 수행해 증거와 데이터를 기반으로 기능 설계 결정을 내릴 수 있습니다. 자세한 내용은 [CloudWatch Evidently를 통해 출시 및 A/B 실험 수행](#)(CloudWatch 설명서)를 참조하세요.

## Amazon CloudWatch Logs를 사용한 애플리케이션 로깅 및 모니터링

[Amazon CloudWatch Logs](#)는 확장성이 뛰어난 단일 서비스에서 사용하는 모든 시스템, 애플리케이션 및 AWS 서비스에서 로그를 중앙 집중화할 수 있습니다. 그런 다음 로그를 쉽게 보고, 특정 오류 코드 또는 패턴이 있는지 검색하고, 특정 필드를 기반으로 필터링하거나, 향후 분석을 위해 안전하게 보관할 수 있습니다. 소스와 관계없이 모든 로그 이벤트를 시간순으로 정렬된 일관된 단일 이벤트 흐름으로 볼 수 있습니다. 쿼리하고 정렬하고, 특정 필드별로 그룹화하고, 사용자 지정 계산을 생성하고, 대시보드에서 로그 데이터를 시각화할 수 있습니다.

### CloudWatch Logs 사용

CloudWatch Logs에서 로그 이벤트는 로그 스트림과 로그 그룹으로 구성됩니다. 로그 스트림은 동일한 소스를 공유하는 로그 이벤트 시퀀스입니다. 보다 구체적으로 말하자면, 로그 스트림은 모니터링 중인

애플리케이션 인스턴스나 리소스에서 나온 이벤트의 시퀀스를 표시하는 데 주로 사용됩니다. 로그 그룹은 동일한 보존 기간, 모니터링 및 액세스 제어 설정을 공유하는 하나 이상의 로그 스트림을 정의합니다. 각 로그 스트림은 적어도 하나의 로그 그룹에 속해야 합니다. 자세한 내용은 [로그 그룹 및 로그 스트림 작업](#)(CloudWatch Logs 설명서)을 참조하세요.

CloudWatch 로그 인사이트를 사용하면 Amazon CloudWatch Logs 내 로그 데이터를 검색해 분석할 수 있습니다. 운영상의 문제에 보다 효율적이고 효과적으로 대처할 수 있도록 쿼리를 수행할 수 있습니다. 문제가 발생하면 CloudWatch Logs Insights를 사용해 잠재적인 원인을 식별하고 배포된 수정 사항을 확인할 수 있습니다. 자세한 내용은 [CloudWatch Logs Insights를 사용한 로그 분석](#)(CloudWatch Logs 설명서)을 참조하세요.

지표 필터를 한 개 이상 생성하여 CloudWatch Logs로 들어오는 로그 데이터를 검색하고 필터링할 수 있습니다. 지표 필터는 CloudWatch Logs 로그로 전송될 때 로그 데이터에서 검색할 단어와 패턴을 정의합니다. CloudWatch Logs는 이러한 지표 필터를 사용하여 로그 데이터를 그래프로 나타내거나 경보를 설정할 수 있는 숫자 CloudWatch 지표로 전환합니다. 자세한 내용은 [필터를 사용하여 로그 이벤트에서 지표 생성](#)(CloudWatch Logs 설명서)을 참조하세요.

## CloudWatch Logs의 사용 사례

- CloudTrail 로그 모니터링 – CloudWatch에서 경보를 생성하고, CloudTrail에서 포착된 특정 API 활동에 대한 알림을 받고, 이러한 알림을 사용하여 문제 해결을 수행할 수 있습니다. 자세한 내용은 [Sending CloudTrail Events to CloudWatch Logs](#)(CloudTrail 설명서)를 참조하세요.
- AWS API 호출 로깅 - 타사 모니터링 솔루션을 사용하는 경우 CloudWatch Logs를 사용하여 AWS API 호출을 로깅할 수 있습니다. 타사 모니터링 서비스를 설정하여 이 로그와 애플리케이션 수준 API를 평가합니다.
- 로그 보존 구성 - CloudWatch Logs의 로그는 기본적으로 로그는 무기한으로 보존되며 만료되지 않습니다. 로그 그룹별로 보존 정책을 조정하거나 무기한 보존을 유지하거나 보존 기간(1일~10년)을 선택할 수 있습니다.
- 로그 아카이브 및 저장 - CloudWatch Logs를 사용하여 내구성이 뛰어난 스토리지에 로그 데이터를 저장할 수 있습니다. CloudWatch Logs 에이전트는 교체된 로그 데이터와 교체되지 않은 로그 데이터를 모두 로그 서비스로 전송합니다. 그런 다음 필요할 때 원시 로그 데이터에 액세스할 수 있습니다.

## VPC Flow Logs를 사용하여 애플리케이션 로깅 및 모니터링

[VPC 흐름 로그](#)는 VPC의 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처하는 데 사용할 수 있는 Amazon Virtual Private Cloud(VPC)의 기능입니다.

## VPC Flow Logs 사용

Virtual Private Cloud(VPC), 서브넷 또는 네트워크 인터페이스에 대한 흐름 로그를 생성할 수 있습니다. 서브넷이나 VPC에 대한 흐름 로그를 생성할 경우, VPC 또는 서브넷의 각 네트워크 인터페이스가 모니터링됩니다. 자세한 내용은 [흐름 로그 작업](#)(Amazon VPC 설명서)을 참조하세요.

모니터링된 네트워크 인터페이스의 흐름 로그 데이터는 흐름 로그 레코드로 기록됩니다. 흐름 로그 레코드는 VPC에 네트워크 흐름을 나타냅니다. 기본적으로 각 레코드는 집계 간격 내에서 발생하는 네트워크 IP 트래픽 흐름을 캡처합니다. 각 레코드는 필드가 공백으로 구분되어 있는 문자열입니다. 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다. 흐름 로그를 생성할 때 흐름 로그 레코드의 기본 형식을 사용하거나 사용자 지정 형식을 지정할 수 있습니다. 자세한 내용은 [흐름 로그 레코드의 예](#)(Amazon VPC 설명서)를 참조하세요.

흐름 로그는 다음 정보를 캡처하지 않습니다.

- 인스턴스가 Amazon 도메인 이름 시스템(DNS) 서버에 연결할 때 생성한 트래픽. 자체 DNS 서버를 사용할 경우 DNS 서버에 대한 모든 트래픽은 기록됩니다.
- Amazon Windows 라이선스 인증을 위해 Windows 인스턴스에서 생성한 트래픽.
- 인스턴스 메타데이터를 위해 254.169.254와 주고받는 트래픽.
- Amazon Time Sync Service를 위해 254.169.123과 주고받는 트래픽.
- Dynamic Host Configuration Protocol(DHCP) 트래픽.
- 기본 VPC 라우터의 예약된 IP 주소로 보내는 트래픽.
- 엔드포인트 네트워크 인터페이스와 Network Load Balancer 네트워크 인터페이스 간의 트래픽.

흐름 로그 데이터는 Amazon CloudWatch Logs를 포함한 여러 AWS 서비스에 게시될 수 있습니다. 흐름 로그를 생성한 후에는 구성된 로그 그룹의 CloudWatch Logs에서 흐름 로그 레코드를 검색하고 볼 수 있습니다. 자세한 내용은 [CloudWatch Logs에 흐름 로그 게시](#)(Amazon VPC 설명서)를 참조하세요.

흐름 로그 데이터는 네트워크 트래픽 경로 외부에서 수집되므로 네트워크 처리량이나 지연 시간에 영향을 주지 않습니다. 네트워크 성능에 영향을 주지 않고 흐름 로그를 생성하거나 삭제할 수 있습니다.

## VPC Flow Logs 사용 사례

- 지나치게 제한적인 보안 그룹 규칙 진단
- 애플리케이션 인스턴스에 도달하는 트래픽 모니터링
- 트래픽 방향 결정

# AWS X-Ray를 사용하여 애플리케이션 로깅 및 모니터링

[AWS X-Ray](#)는 애플리케이션이 처리하는 요청에 대한 데이터를 수집하며, 해당 데이터를 보고, 필터링하고, 인사이트를 얻어 최적화에 대한 문제와 기회를 파악하는 데 도움이 됩니다.

## X-Ray 사용

AWS X-Ray는 애플리케이션에서 추적을 받고, X-Ray와 통합된 경우 애플리케이션이 사용하는 AWS 서비스에서도 추적을 받습니다. X-Ray는 요청이 애플리케이션 구성 요소를 통해 흐를 때 [서비스 그래프](#)에서 요청을 샘플링하고 시각화합니다. X-Ray는 추적 식별자를 생성하므로 요청이 여러 구성 요소를 통과할 때 요청을 상호 연관시킬 수 있으므로 요청을 처음부터 끝까지 볼 수 있습니다. 요청의 특성을 고유하게 검색하고 식별하는 데 도움이 되는 주석과 메타데이터를 포함하여 이를 더욱 개선할 수 있습니다.

애플리케이션의 각 서버 또는 엔드포인트를 X-Ray로 구성하는 것이 좋습니다. X-Ray는 X-Ray 서비스를 호출하여 애플리케이션 코드에서 구현됩니다. X-Ray는 또한 자동으로 X-Ray에 데이터를 전송하는 계층 클라이언트를 포함하여 여러 언어에 대한 AWS SDK를 제공합니다. X-Ray SDK는 다른 서비스(예: HTTP, MySQL, PostgreSQL 또는 MongoDB)를 직접적으로 호출하는 데 사용되는 공통 라이브러리에 대한 패치를 제공합니다.

자세한 내용은 [Tracing applications with AWS X-Ray](#)(AWS 권장 가이드)를 참조하세요.

## X-Ray의 사용 사례

- 애플리케이션 분석 및 디버그 - 추적 데이터는 요청을 종합적으로 파악하여 병목 현상을 식별하고 문제를 해결함으로써 애플리케이션을 디버깅하는 데 도움이 될 수 있습니다. X-Ray [서비스 맵](#)은 오류가 발생하는 위치, 지연 시간이 긴 연결 또는 실패한 요청 추적을 식별하는 데 도움이 되는 시각적 도구입니다.
- 성능 분석 - [분석 콘솔](#)은 트레이스 데이터를 해석하여 애플리케이션과 기본 서비스의 성능을 빠르게 파악할 수 있는 대화형 도구입니다. 콘솔을 사용하면 트레이스를 탐색, 분석 및 시각화할 수 있습니다. 또한 근본 원인 분석을 위해 다양한 조건의 트레이스 세트를 비교할 수 있습니다.

## 자주 묻는 질문

### 현재 사용 중인 모니터링 서비스를 사용할 수 있나요?

[Amazon CloudWatch](#)는 DevOps 엔지니어, 개발자, 사이트 신뢰성 엔지니어(SRE), IT 관리자 및 애플리케이션 소유자를 위해 구축된 모니터링 및 관찰성 서비스입니다. 이는 애플리케이션을 모니터링하고, 시스템 전반의 성능 변화에 대응하고, 리소스 사용률을 최적화하는 데 도움이 되는 데이터와 실행 가능한 인사이트를 제공합니다. 하지만 모니터링 서비스가 이미 확립되어 있다면 교체하지 않아도 됩니다.

### 로그 파일이 변조되지 않도록 하려면 어떻게 해야 하나요?

로그 파일 무결성 검증을 활성화할 수 있습니다. 전용 AWS 계정에 로그를 관리 및 저장하고 해당 계정에 대한 액세스를 제한하는 것이 좋습니다. 자세한 내용은 이 가이드의 [CloudTrail 사용](#)을 참조하세요.

### 각 애플리케이션마다 별도의 로그 파일을 유지해야 하나요?

아니요, 여러 애플리케이션의 로그 데이터를 동일한 로그 파일로 통합할 수 있습니다. 하지만 각 애플리케이션의 고유 식별자가 로그 스트림에 기록되어 있는지 확인해야 합니다.



# 리소스

## AWS 설명서

- [AWS CloudTrail 설명서](#)
- [AWS 클라우드Watch 설명서](#)
- [AWS 클라우드Watch Logs 설명서](#)
- [Amazon VPC Flow Logs 설명서](#)
- [AWS X-Ray 설명서](#)
- [Amazon CloudWatch를 사용한 로깅 및 모니터링 설계 및 구현\(AWS 권장 가이드\)](#)

## AWS 마케팅

- [AWS CloudTrail](#)
- [Amazon CloudWatch](#)
- [AWS의 중앙 집중식 로깅\(AWS 솔루션\)](#)
- [모니터링 및 관찰성\(AWS 클라우드 운영\)](#)
- [애플리케이션을 효과적으로 모니터링하는 방법\(AWS 스타트업\)](#)

## 문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 [RSS 피드](#)를 구독하세요.

변경 사항	설명	날짜
<a href="#">최초 게시</a>	—	2023년 1월 6일

# AWS 권장 가이드 용어집

다음은 AWS 권장 가이드에서 제공하는 전략, 가이드, 패턴 등에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하세요.

## 숫자

### 7가지 전략

애플리케이션을 클라우드로 이전하기 위한 7가지 일반적인 마이그레이션 전략 이러한 전략은 Gartner가 2011년에 파악한 5가지 전략을 기반으로 하며 다음으로 구성됩니다.

- 리팩터링/리아키텍트 - 클라우드 네이티브 기능을 최대한 활용하여 애플리케이션을 이동하고 해당 아키텍처를 수정함으로써 민첩성, 성능 및 확장성을 개선합니다. 여기에는 일반적으로 운영 체제와 데이터베이스 이식이 포함됩니다. 예를 들어, 온프레미스 Oracle 데이터베이스를 Amazon Aurora PostgreSQL 호환 버전으로 마이그레이션합니다.
- 리플랫폼(리프트 앤드 리세이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예를 들어, 온프레미스 Oracle 데이터베이스를 AWS 클라우드의 Amazon RDS for Oracle로 마이그레이션합니다.
- 재구매(드롭 앤드 슝) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예를 들어, 고객 관계 관리(CRM) 시스템을 Salesforce.com으로 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예를 들어, 온프레미스 Oracle 데이터베이스를 AWS 클라우드의 EC2 인스턴스에 있는 Oracle로 마이그레이션합니다.
- 재배포(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 이 마이그레이션 시나리오는 온프레미스 환경과 AWS 간의 가상 머신 호환성 및 워크로드 이동성을 지원하는 AWS의 VMware Cloud에 한정됩니다. 인프라를 AWS의 VMware Cloud로 마이그레이션할 때 온프레미스 데이터 센터에서 VMware Cloud Foundation 기술을 사용할 수 있습니다. 예를 들어, Oracle 데이터베이스를 호스팅하는 하이퍼바이저를 AWS의 VMware Cloud로 재배포합니다.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중에 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

# A

## ABAC

[속성 기반 액세스](#) 제어를 참조하십시오.

## 추상화된 서비스

[매니지드 서비스를](#) 참조하십시오.

## 산

[원자성, 일관성, 격리성, 내구성을](#) 참조하십시오.

## 능동-능동 마이그레이션

양방향 복제 도구 또는 이중 쓰기 작업을 사용하여 소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되고, 두 데이터베이스 모두 마이그레이션 중 연결 애플리케이션의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 이 방법은 일회성 전환이 필요한 대신 소규모의 제어된 배치로 마이그레이션을 지원합니다. [더 유연하지만 액티브-패시브 마이그레이션보다 더 많은 작업이 필요합니다.](#)

## 능동-수동 마이그레이션

소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되지만 소스 데이터베이스만 연결 애플리케이션의 트랜잭션을 처리하고 데이터는 대상 데이터베이스로 복제되는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

## 집계 함수

행 그룹에서 연산을 수행하고 그룹에 대한 단일 반환값을 계산하는 SQL 함수입니다. 집계 함수의 예로는 `MAX` 및 `SUM` 등이 있습니다.

## AI

[인공 지능을](#) 참조하십시오.

## AIOps

[인공 지능 운영을](#) 참조하십시오.

## 익명화

데이터세트에서 개인 정보를 영구적으로 삭제하는 프로세스입니다. 익명화는 개인 정보 보호에 도움이 될 수 있습니다. 익명화된 데이터는 더 이상 개인 데이터로 간주되지 않습니다.

## 안티 패턴

솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다.

## 애플리케이션 제어

시스템을 멀웨어로부터 보호하기 위해 승인된 애플리케이션만 사용할 수 있는 보안 접근 방식입니다.

## 애플리케이션 포트폴리오

애플리케이션 구축 및 유지 관리 비용과 애플리케이션의 비즈니스 가치를 비롯하여 조직에서 사용하는 각 애플리케이션에 대한 세부 정보 모음입니다. 이 정보는 [포트폴리오 검색 및 분석 프로세스](#)의 핵심이며 마이그레이션, 현대화 및 최적화할 애플리케이션을 식별하고 우선순위를 정하는 데 도움이 됩니다.

## 인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 [What is Artificial Intelligence?](#)를 참조하세요.

## 인공 지능 운영(AIOps)

기계 학습 기법을 사용하여 운영 문제를 해결하고, 운영 인시던트 및 사용자 개입을 줄이고, 서비스 품질을 높이는 프로세스입니다. AWS 마이그레이션 전략에서 AIOps가 사용되는 방법에 대한 자세한 내용은 [운영 통합 가이드](#)를 참조하세요.

## 비대칭 암호화

한 쌍의 키, 즉 암호화를 위한 퍼블릭 키와 복호화를 위한 프라이빗 키를 사용하는 암호화 알고리즘입니다. 퍼블릭 키는 복호화에 사용되지 않으므로 공유할 수 있지만 프라이빗 키에 대한 액세스는 엄격히 제한되어야 합니다.

## 원자성, 일관성, 격리성, 내구성(ACID)

오류, 정전 또는 기타 문제가 발생한 경우에도 데이터베이스의 데이터 유효성과 운영 신뢰성을 보장하는 소프트웨어 속성 세트입니다.

## ABAC(속성 기반 액세스 제어)

부서, 직무, 팀 이름 등의 사용자 속성을 기반으로 세분화된 권한을 생성하는 방식입니다. 자세한 내용은 AWS Identity and Access Management(IAM) 설명서의 [AWS용 ABAC란 무엇입니까?](#)를 참조하세요.

## 신뢰할 수 있는 데이터 소스

가장 신뢰할 수 있는 정보 소스로 간주되는 기본 버전의 데이터를 저장하는 위치입니다. 익명화, 편집 또는 가명화와 같은 데이터 처리 또는 수정의 목적으로 신뢰할 수 있는 데이터 소스의 데이터를 다른 위치로 복사할 수 있습니다.

### 가용 영역

다른 가용 영역에 장애가 발생할 경우 분리되도록 설계된 AWS 리전 내의 개별적인 지점으로, 같은 리전 내의 다른 가용 영역에 비해 저렴하고 지연 시간이 짧은 네트워크 연결을 제공합니다.

### AWS Cloud Adoption Framework(AWS CAF)

조직이 클라우드로 성공적으로 전환하기 위한 효율적이고 효과적인 계획을 개발하는 데 도움이 되는 AWS의 지침 및 모범 사례 프레임워크입니다. AWS CAF는 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영 관점이라는 6가지 중점 영역으로 지침을 구성합니다. 비즈니스, 사람 및 거버넌스 관점은 비즈니스 기술과 프로세스에 초점을 맞추고, 플랫폼, 보안 및 운영 관점은 전문 기술과 프로세스에 중점을 둡니다. 예를 들어, 사람 관점은 인사(HR), 직원 배치 기능 및 인력 관리를 담당하는 이해관계자를 대상으로 합니다. 이러한 관점에서 AWS CAF는 조직이 클라우드를 성공적으로 채택할 수 있도록 인력 개발, 교육 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 [AWS CAF 웹 사이트](#)와 [AWS CAF 백서](#)를 참조하세요.

### AWS Workload Qualification Framework(AWS WQF)

데이터베이스 마이그레이션 워크로드를 평가하고, 마이그레이션 전략을 추천하고, 작업 추정치를 제공하는 도구입니다. AWS WQF는 AWS Schema Conversion Tool(AWS SCT)에 포함되어 있으며, 데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

## B

### BCP

[비즈니스 연속성 계획을](#) 참조하십시오.

### 동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그온 시도, 의심스러운 API 호출 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 [Data in a behavior graph](#)를 참조하세요.

## 빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. [엔디안도](#) 참조하십시오.

## 바이너리 분류

바이너리 결과(가능한 두 클래스 중 하나)를 예측하는 프로세스입니다. 예를 들어, ML 모델이 '이 이메일이 스팸인가요, 스팸이 아닌가요?', '이 제품은 책임가요, 자동차인가요?' 등의 문제를 예측해야 할 수 있습니다.

## 블룸 필터

요소가 세트의 멤버인지 여부를 테스트하는 데 사용되는 메모리 효율성이 높은 확률론적 데이터 구조입니다.

## 브랜치

코드 리포지토리의 포함된 영역입니다. 리포지토리에 생성되는 첫 번째 브랜치가 기본 브랜치입니다. 기존 브랜치에서 새 브랜치를 생성한 다음 새 브랜치에서 기능을 개발하거나 버그를 수정할 수 있습니다. 기능을 구축하기 위해 생성하는 브랜치를 일반적으로 기능 브랜치라고 합니다. 기능을 출시할 준비가 되면 기능 브랜치를 기본 브랜치에 다시 병합합니다. 자세한 내용은 [브랜치 정보](#) (GitHub 문서) 를 참조하십시오.

## 브레이크 글래스 액세스

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스 권한이 없는 데이터에 빠르게 액세스할 수 있는 AWS 계정 있는 수단입니다. 자세한 내용은 Well-Architected AWS 지침의 [브레이크 글래스 절차 구현](#) 표시기를 참조하십시오.

## 브라운필드 전략

사용자 환경의 기존 인프라 시스템 아키텍처에 브라운필드 전략을 채택할 때는 현재 시스템 및 인프라의 제약 조건을 중심으로 아키텍처를 설계합니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 [그린필드](#) 전략을 혼합할 수 있습니다.

## 버퍼 캐시

가장 자주 액세스하는 데이터가 저장되는 메모리 영역입니다.

## 사업 역량

기업이 가치를 창출하기 위해 하는 일(예: 영업, 고객 서비스 또는 마케팅)입니다. 마이크로서비스 아키텍처 및 개발 결정은 비즈니스 역량에 따라 이루어질 수 있습니다. 자세한 내용은 백서의 [컨테이너화된 마이크로서비스 실행](#) AWS의 [비즈니스 역량 중심의 구성화](#) 섹션을 참조하세요.

## 비즈니스 연속성 계획(BCP)

대규모 마이그레이션과 같은 중단 이벤트가 운영에 미치는 잠재적 영향을 해결하고 비즈니스가 신속하게 운영을 재개할 수 있도록 지원하는 계획입니다.

## C

### CAF

[클라우드 채택 프레임워크를 참조하십시오AWS.](#)

### CCoE

[클라우드 센터 오브 엑셀런스를 참조하십시오.](#)

### CDC

[변경 데이터 캡처를 참조하십시오.](#)

### 변경 데이터 캡처(CDC)

데이터베이스 테이블과 같은 데이터 소스의 변경 내용을 추적하고 변경 사항에 대한 메타데이터를 기록하는 프로세스입니다. 대상 시스템의 변경 내용을 감사하거나 복제하여 동기화를 유지하는 등의 다양한 용도로 CDC를 사용할 수 있습니다.

### 카오스 엔지니어링

시스템의 복원력을 테스트하기 위해 의도적으로 장애나 장애를 일으키는 이벤트를 발생시키는 행위 [AWS Fault Injection Service\(AWS FIS\)](#) 를 사용하여 AWS 워크로드에 스트레스를 주는 실험을 수행하고 응답을 평가할 수 있습니다.

### CI/CD

[지속적 통합 및 지속적 전달을 참조하십시오.](#)

### 분류

예측을 생성하는 데 도움이 되는 분류 프로세스입니다. 분류 문제에 대한 ML 모델은 이산 값을 예측합니다. 이산 값은 항상 서로 다릅니다. 예를 들어, 모델이 이미지에 자동차가 있는지 여부를 평가해야 할 수 있습니다.

### 클라이언트측 암호화

데이터를 대상 AWS 서비스에서 수신하기 전에 로컬에서 암호화합니다.



## 클라우드 혁신 센터(CCoE)

클라우드 모범 사례 개발, 리소스 동원, 마이그레이션 타임라인 설정, 대규모 혁신을 통한 조직 선도 등 조직 전체에서 클라우드 채택 노력을 추진하는 다분야 팀입니다. 자세한 내용은 AWS 클라우드 엔터프라이즈 전략 블로그의 [CCoE 게시물](#)을 참조하세요.

## 클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 [엣지 컴퓨팅](#) 기술과 연결됩니다.

## 클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 [클라우드 운영 모델 구축](#)을 참조하세요.

## 클라우드 채택 단계

조직이 AWS 클라우드로 마이그레이션할 때 일반적으로 거치는 4단계는 다음과 같습니다.

- 프로젝트 - 개념 증명 및 학습 목적으로 몇 가지 클라우드 관련 프로젝트 실행
- 기반 - 클라우드 채택 확장을 위한 기초 투자(예: 랜딩 존 생성, CCoE 정의, 운영 모델 구축)
- 마이그레이션 - 개별 애플리케이션 마이그레이션
- Re-invention - 제품 및 서비스 최적화와 클라우드 혁신

이러한 단계는 Stephen Orban이 AWS Cloud Enterprise Strategy Blog의 [The Journey Toward Cloud-First & the Stages of Adoption](#) 블로그 게시물에서 정의했습니다. AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 [마이그레이션 준비 가이드](#)를 참조하세요.

## CMDB

[구성 관리 데이터베이스](#)를 참조하십시오.

## 코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반 클라우드 리포지토리에는 또는 이 포함됩니다 GitHub . AWS CodeCommit 코드의 각 버전을 브랜치라고 합니다. 마이크로서비스 구조에서 각 리포지토리는 단일 기능 전용입니다. 단일 CI/CD 파이프라인은 여러 리포지토리를 사용할 수 있습니다.

## 콜드 캐시

비어 있거나, 제대로 채워지지 않았거나, 오래되었거나 관련 없는 데이터를 포함하는 버퍼 캐시입니다. 주 메모리나 디스크에서 데이터베이스 인스턴스를 읽어야 하기 때문에 성능에 영향을 미치며, 이는 버퍼 캐시에서 읽는 것보다 느립니다.

## 콜드 데이터

거의 액세스되지 않고 일반적으로 과거 데이터인 데이터. 이런 종류의 데이터를 쿼리할 때는 일반적으로 느린 쿼리가 허용됩니다. 이 데이터를 성능이 낮고 비용이 저렴한 스토리지 계층 또는 클래스로 옮기면 비용을 절감할 수 있습니다.

## 컴퓨터 비전

기계가 이미지 속 사람, 장소, 사물을 인간 수준 이상의 정확도로 식별하는 데 사용하는 AI 분야입니다. 딥 러닝 모델로 구축되는 경우가 많으며 단일 이미지 또는 일련의 이미지에서 유용한 정보를 자동으로 추출, 분석, 분류 및 이해합니다.

## 구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션의 포트폴리오 검색 및 분석 단계에서 CMDB의 데이터를 사용합니다.

## 규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 수정 작업 모음입니다. YAML 템플릿을 사용하여 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 규정 준수 팩을 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 [Conformance packs](#)를 참조하세요.

## 지속적 통합 및 지속적 전달(CI/CD)

소프트웨어 릴리스 프로세스의 소스, 빌드, 테스트, 스테이징 및 프로덕션 단계를 자동화하는 프로세스입니다. CI/CD는 일반적으로 파이프라인으로 설명됩니다. CI/CD를 통해 프로세스를 자동화하고, 생산성을 높이고, 코드 품질을 개선하고, 더 빠르게 제공할 수 있습니다. 자세한 내용은 [지속적 전달의 이점](#)을 참조하세요. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 [지속적 전달\(Continuous Delivery\)](#)과 [지속적인 개발](#)을 참조하세요.

# D

## 저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

## 데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리

전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected Framework 보안 원칙의 구성 요소입니다. 자세한 내용은 [데이터 분류](#)를 참조하세요.

## 데이터 드리프트

프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습니다.

## 전송 중 데이터

네트워크를 통과하고 있는 데이터입니다. 네트워크 리소스 사이를 이동 중인 데이터를 예로 들 수 있습니다.

## 데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. AWS 클라우드에서 데이터 최소화를 실천하면 개인 정보 보호 위험, 비용 및 분석에 따른 탄소 발자국을 줄일 수 있습니다.

## 데이터 경계

신뢰할 수 있는 ID만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경 내 일련의 예방 가드레일입니다. 자세한 내용은 [데이터 경계 구축](#)을 참조하십시오.

## AWS

## 데이터 사전 처리

원시 데이터를 ML 모델이 쉽게 구문 분석할 수 있는 형식으로 변환하는 것입니다. 데이터를 사전 처리한다는 것은 특정 열이나 행을 제거하고 누락된 값, 일관성이 없는 값 또는 중복 값을 처리함을 의미할 수 있습니다.

## 데이터 출처

라이프사이클 전반에 걸쳐 데이터의 출처와 기록을 추적하는 프로세스(예: 데이터 생성, 전송, 저장 방법).

## 데이터 주체

데이터를 수집 및 처리하는 개인입니다.

## 데이터 웨어하우스

분석과 같은 비즈니스 인텔리전스를 지원하는 데이터 관리 시스템. 데이터 웨어하우스에는 일반적으로 대량의 과거 데이터가 포함되며 일반적으로 쿼리 및 분석에 사용됩니다.

## 데이터 정의 언어(DDL)

데이터베이스에서 테이블 및 객체의 구조를 만들거나 수정하기 위한 명령문 또는 명령입니다.

## 데이터베이스 조작 언어(DML)

데이터베이스에서 정보를 수정(삽입, 업데이트 및 삭제)하기 위한 명령문 또는 명령입니다.

## DDL

[데이터베이스 정의 언어를](#) 참조하십시오.

## 딥 앙상블

예측을 위해 여러 딥 러닝 모델을 결합하는 것입니다. 딥 앙상블을 사용하여 더 정확한 예측을 얻거나 예측의 불확실성을 추정할 수 있습니다.

## 딥 러닝

여러 계층의 인공 신경망을 사용하여 입력 데이터와 관심 대상 변수 간의 매핑을 식별하는 ML 하위 분야입니다.

## defense-in-depth

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. AWS에서 이 전략을 채택하면 AWS Organizations 구조의 다양한 계층에 여러 제어 기능을 추가하여 리소스를 보호할 수 있습니다. 예를 들어, defense-in-depth 접근 방식에는 다단계 인증, 네트워크 분할 및 암호화를 결합할 수 있습니다.

## 위임된 관리자

AWS Organizations에서 호환되는 서비스는 AWS 멤버 계정을 등록하여 조직의 계정을 관리하고 해당 서비스에 대한 권한을 관리할 수 있습니다. 이러한 계정을 해당 서비스의 위임된 관리자라고 합니다. 자세한 내용과 호환되는 서비스 목록은 AWS Organizations 설명서의 [AWS Organizations와 함께 사용할 수 있는 AWS 서비스](#)를 참조하세요.

## 배포

대상 환경에서 애플리케이션, 새 기능 또는 코드 수정 사항을 사용할 수 있도록 하는 프로세스입니다. 배포에는 코드 베이스의 변경 사항을 구현한 다음 애플리케이션 환경에서 해당 코드베이스를 구축하고 실행하는 작업이 포함됩니다.

## 개발 환경

[환경을](#) 참조하십시오.

## 탐지 제어

이벤트 발생 후 탐지, 기록 및 알림을 수행하도록 설계된 보안 제어입니다. 이러한 제어는 기존의 예방적 제어를 우회한 보안 이벤트를 알리는 2차 방어선입니다. 자세한 내용은 [Implementing security controls on AWS의 Detective controls](#)를 참조하세요.

## 개발 가치 흐름 매핑 (DVSM)

소프트웨어 개발 라이프사이클에서 속도와 품질에 부정적인 영향을 미치는 제약 조건을 식별하고 우선 순위를 지정하는 데 사용되는 프로세스입니다. DVSM은 원래 린 제조 방식을 위해 설계된 가치 흐름 매핑 프로세스를 확장합니다. 소프트웨어 개발 프로세스를 통해 가치를 창출하고 이동하는 데 필요한 단계와 팀에 중점을 둡니다.

## 디지털 트윈

건물, 공장, 산업 장비 또는 생산 라인과 같은 실제 시스템을 가상으로 표현한 것입니다. 디지털 트윈은 예측 유지 보수, 원격 모니터링, 생산 최적화를 지원합니다.

## 치수 표

[스타 스키마에서](#) 팩트 테이블의 양적 데이터에 대한 데이터 속성을 포함하는 작은 테이블입니다. 차원 테이블 속성은 일반적으로 텍스트처럼 동작하는 텍스트 필드 또는 불연속형 숫자입니다. 이러한 속성은 일반적으로 쿼리 제한, 필터링 및 결과 집합 레이블 지정에 사용됩니다.

## 재해

워크로드 또는 시스템이 기본 배포 위치에서 비즈니스 목표를 달성하지 못하게 방해하는 이벤트입니다. 이러한 이벤트는 자연재해, 기술적 오류, 의도하지 않은 구성 오류 또는 멀웨어 공격과 같은 사람의 행동으로 인한 결과일 수 있습니다.

## 재해 복구(DR)

[재해로 인한 다운타임과 데이터 손실을 최소화하기 위해 사용하는 전략과 프로세스입니다.](#) 자세한 내용은 AWS Well-Architected Framework의 [AWS 기반 워크로드의 재해 복구: 클라우드에서의 재해 복구](#)를 참조하세요.

## DML

[데이터베이스 조작 언어](#)를 참조하십시오.

## 도메인 기반 설계

구성 요소를 각 구성 요소가 제공하는 진화하는 도메인 또는 핵심 비즈니스 목표에 연결하여 복잡한 소프트웨어 시스템을 개발하는 접근 방식입니다. 이 개념은 에릭 에반스에 의해 그의 저서인 도

메인 기반 디자인: 소프트웨어 중심의 복잡성 해결(Boston: Addison-Wesley Professional, 2003)에서 소개되었습니다. Strangler Fig 패턴과 함께 도메인 기반 설계를 사용하는 방법에 대한 자세한 내용은 [컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET\(ASMX\) 웹 서비스를 점진적으로 현대화하는 방법](#)을 참조하세요.

## DR

[재해 복구를](#) 참조하십시오.

### 드리프트 감지

기존 구성으로부터의 편차 추적 예를 들어 [시스템 리소스의 편차를 감지하는 AWS CloudFormation](#) 데 사용하거나 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 [착륙 지대의 변경을 탐지하는 AWS Control Tower](#) 데 사용할 수 있습니다.

## DVSM

[개발 가치 흐름 매핑](#)을 참조하십시오.

## E

### EDA

[탐색적 데이터 분석](#)을 참조하십시오.

### 엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 [클라우드 컴퓨팅과](#) 비교할 때 엣지 컴퓨팅은 통신 대기 시간을 줄이고 응답 시간을 개선할 수 있습니다.

### 암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 암호문으로 변환하는 컴퓨팅 프로세스입니다.

### 암호화 키

암호화 알고리즘에 의해 생성되는 무작위 비트의 암호화 문자열입니다. 키의 길이는 다양할 수 있으며 각 키는 예측할 수 없고 고유하게 설계되었습니다.

### 엔디안

컴퓨터 메모리에 바이트가 저장되는 순서입니다. 빅 엔디안 시스템은 가장 중요한 바이트를 먼저 저장합니다. 리틀 엔디안 시스템은 가장 덜 중요한 바이트를 먼저 저장합니다.

## 엔드포인트

[서비스](#) 엔드포인트를 참조하십시오.

### 엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. AWS PrivateLink를 사용하여 엔드포인트 서비스를 생성하고 다른 AWS 계정 또는 AWS Identity and Access Management(IAM) 보안 주체에게 권한을 부여할 수 있습니다. 이러한 계정 또는 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 설명서의 [엔드포인트 서비스 생성](#)을 참조하세요.

### 봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service(AWS KMS) 설명서의 [Envelope encryption](#)을 참조하세요.

### 환경

실행 중인 애플리케이션의 인스턴스입니다. 다음은 클라우드 컴퓨팅의 일반적인 환경 유형입니다.

- 개발 환경 - 애플리케이션 유지 관리를 담당하는 핵심 팀만 사용할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. 개발 환경은 변경 사항을 상위 환경으로 승격하기 전에 테스트하는 데 사용됩니다. 이러한 유형의 환경을 테스트 환경이라고도 합니다.
- 하위 환경 - 초기 빌드 및 테스트에 사용되는 환경을 비롯한 애플리케이션의 모든 개발 환경입니다.
- 프로덕션 환경 - 최종 사용자가 액세스할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. CI/CD 파이프라인에서 프로덕션 환경이 마지막 배포 환경입니다.
- 상위 환경 - 핵심 개발 팀 이외의 사용자가 액세스할 수 있는 모든 환경입니다. 프로덕션 환경, 프로덕션 이전 환경 및 사용자 수용 테스트를 위한 환경이 여기에 포함될 수 있습니다.

### 에픽

애자일 방법론에서 작업을 구성하고 우선순위를 정하는 데 도움이 되는 기능적 범주입니다. 에픽은 요구 사항 및 구현 작업에 대한 개괄적인 설명을 제공합니다. 예를 들어, AWS CAF 보안 에픽에는 ID 및 액세스 관리, 탐지 제어, 인프라 보안, 데이터 보호 및 인시던트 대응 등이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 [프로그램 구현 가이드](#)를 참조하세요.

### 탐색 데이터 분석(EDA)

데이터 세트를 분석하여 주요 특성을 파악하는 프로세스입니다. 데이터를 수집 또는 집계한 다음 초기 조사를 수행하여 패턴을 찾고, 이상을 탐지하고, 가정을 확인합니다. EDA는 요약 통계를 계산하고 데이터 시각화를 생성하여 수행됩니다.

## F

### 팩트 테이블

[스타 스키마의](#) 중앙 테이블. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블에는 측정값이 포함된 열과 차원 테이블의 외부 키가 포함된 열 등 두 가지 유형의 열이 포함됩니다.

### 빨리 실패하세요

빈번하고 점진적인 테스트를 통해 개발 라이프사이클을 단축하는 철학. 이는 애자일 접근 방식의 중요한 부분입니다.

### 장애 격리 경계

장애 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역 AWS 리전, 컨트롤 플레인 또는 데이터 플레인과 같은 경계 AWS 클라우드 자세한 내용은 [AWS 장애 격리](#) 경계를 참조하십시오.

### 기능 브랜치

[브랜치를](#) 참조하십시오.

### 기능

예측에 사용하는 입력 데이터입니다. 예를 들어, 제조 환경에서 기능은 제조 라인에서 주기적으로 캡처되는 이미지일 수 있습니다.

### 기능 중요도

모델의 예측에 특성이 얼마나 중요한지를 나타냅니다. 이는 일반적으로 SHAP(Shapley Additive Descriptions) 및 통합 그래디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 [다음은 AWS 사용한 기계 학습 모델 해석 가능성을](#) 참조하십시오.

### 기능 변환

추가 소스로 데이터를 보강하거나, 값을 조정하거나, 단일 데이터 필드에서 여러 정보 세트를 추출하는 등 ML 프로세스를 위해 데이터를 최적화하는 것입니다. 이를 통해 ML 모델이 데이터를 활용할 수 있습니다. 예를 들어, 날짜 '2021-05-27 00:15:37'을 '2021년', '5월', '목', '15일'로 분류하면 학습 알고리즘이 다양한 데이터 구성 요소와 관련된 미묘한 패턴을 학습하는 데 도움이 됩니다.

### FGAC

[세분화된 액세스 제어](#)를 참조하십시오.



## 세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

### 플래시컷 마이그레이션

단계별 접근 방식 대신 [변경 데이터 캡처를 통한 지속적인 데이터](#) 복제를 통해 최단 시간에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

## G

### 지리적 차단

[지리적 제한](#)을 참조하십시오.

#### 지리적 제한(지리적 차단)

CloudFrontAmazon에서는 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 옵션을 제공합니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 [설명서의 콘텐츠의 지리적 배포 제한](#)을 참조하십시오. CloudFront

### Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 [트렁크 기반 워크플로는](#) 현대적이고 선호되는 접근 방식입니다.

### 브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 [브라운필드](#)라고도 하는 기존 인프라와의 호환성 제한 없이 모든 새로운 기술을 선택할 수 있습니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

### 가드레일

조직 단위(OU) 전체에서 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 중요 규칙입니다. 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책과 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, 이들은, Amazon AWS Config AWS Security Hub GuardDutyAWS Trusted Advisor, Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

# H

## 하

[고가용성을](#) 확인하세요.

### 이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스키마를 변환하는 것은 복잡한 작업일 수 있습니다. AWS는 스키마 변환에 도움이 되는 [AWS SCT](#)를 제공합니다.

### 높은 가용성(HA)

문제나 재해 발생 시 개입 없이 지속적으로 운영할 수 있는 워크로드의 능력. HA 시스템은 자동으로 장애 조치되고, 지속적으로 고품질 성능을 제공하고, 성능에 미치는 영향을 최소화하면서 다양한 부하와 장애를 처리하도록 설계되었습니다.

### 히스토리언 현대화

제조 산업의 요구 사항을 더 잘 충족하도록 운영 기술(OT) 시스템을 현대화하고 업그레이드하는 데 사용되는 접근 방식입니다. 히스토리언은 공장의 다양한 출처에서 데이터를 수집하고 저장하는 데 사용되는 일종의 데이터베이스입니다.

### 동종 데이터베이스 마이그레이션

동일한 데이터베이스 엔진을 공유하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Microsoft SQL Server에서 Amazon RDS for SQL Server로) 동종 마이그레이션은 일반적으로 리호스팅 또는 리플랫폼 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

### 핫 데이터

자주 액세스하는 데이터(예: 실시간 데이터 또는 최근 번역 데이터). 일반적으로 이 데이터에는 빠른 쿼리 응답을 제공하기 위한 고성능 스토리지 계층 또는 클래스가 필요합니다.

### 핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 긴급성 때문에 핫픽스는 일반적으로 일반적인 DevOps 릴리스 워크플로 외부에서 만들어집니다.

## 하이퍼케어 기간

전환 직후 마이그레이션 팀이 문제를 해결하기 위해 클라우드에서 마이그레이션된 애플리케이션을 관리하고 모니터링하는 기간입니다. 일반적으로 이 기간은 1~4일입니다. 하이퍼케어 기간이 끝나면 마이그레이션 팀은 일반적으로 애플리케이션에 대한 책임을 클라우드 운영 팀에 넘깁니다.

## I

### IaC

[인프라를 코드로 보세요.](#)

### ID 기반 정책

하나 이상의 IAM 보안 주체에 연결된 정책으로, AWS 클라우드 환경 내에서 IAM 보안 주체의 권한을 정의합니다.

### 유휴 애플리케이션

90일 동안 평균 CPU 및 메모리 사용량이 5~20%인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하거나 온프레미스에 유지하는 것이 일반적입니다.

## IIoT

[산업용 사물 인터넷을 참조하십시오.](#)

### 불변의 인프라

기존 인프라를 업데이트, 패치 또는 수정하는 대신 프로덕션 워크로드용 새 인프라를 배포하는 모델입니다. [변경 불가능한 인프라는 기본적으로 변경 가능한 인프라보다 더 일관되고 안정적이며 예측 가능합니다.](#) 자세한 내용은 Well-Architected AWS 프레임워크의 [변경 불가능한 인프라를 사용한 배포](#) 모범 사례를 참조하십시오.

### 인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부의 네트워크 연결을 수락, 검사 및 라우팅하는 VPC입니다. [AWS Security Reference Architecture](#)에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

### 중분 마이그레이션

한 번에 전체 전환을 수행하는 대신 애플리케이션을 조금씩 마이그레이션하는 전환 전략입니다. 예를 들어, 처음에는 소수의 마이크로서비스나 사용자만 새 시스템으로 이동할 수 있습니다. 모든 것

이 제대로 작동하는지 확인한 후에는 레거시 시스템을 폐기할 수 있을 때까지 추가 마이크로서비스 또는 사용자를 점진적으로 이동할 수 있습니다. 이 전략을 사용하면 대규모 마이그레이션과 관련된 위험을 줄일 수 있습니다.

## 인프라

애플리케이션의 환경 내에 포함된 모든 리소스와 자산입니다.

### 코드형 인프라(IaC)

구성 파일 세트를 통해 애플리케이션의 인프라를 프로비저닝하고 관리하는 프로세스입니다. IaC는 새로운 환경의 반복 가능성, 신뢰성 및 일관성을 위해 인프라 관리를 중앙 집중화하고, 리소스를 표준화하고, 빠르게 확장할 수 있도록 설계되었습니다.

### 산업용 사물 인터넷(IIoT)

제조, 에너지, 자동차, 의료, 생명과학, 농업 등의 산업 부문에서 인터넷에 연결된 센서 및 디바이스의 사용 자세한 내용은 [산업용 사물 인터넷\(IoT\) 디지털 트랜스포메이션 전략 구축](#)을 참조하세요.

### 검사 VPC

AWS 다중 계정 아키텍처에서 동일한 또는 다른 AWS 리전에 있는 VPC, 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPC입니다. [AWS Security Reference Architecture](#)에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

### 사물 인터넷(IoT)

인터넷이나 로컬 통신 네트워크를 통해 다른 디바이스 및 시스템과 통신하는 센서 또는 프로세서가 내장된 연결된 물리적 객체의 네트워크 자세한 내용은 [IoT란?](#)을 참조하세요.

### 해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 [Machine learning model interpretability with AWS](#)를 참조하세요.

### IoT

[사물 인터넷을 참조하십시오.](#)

### IT 정보 라이브러리(TIL)

IT 서비스를 제공하고 이러한 서비스를 비즈니스 요구 사항에 맞게 조정하기 위한 일련의 모범 사례 ITIL은 ITSM의 기반을 제공합니다.

## IT 서비스 관리(TSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 운영을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 [운영 통합 가이드](#)를 참조하세요.

## ITIL

[IT 정보 라이브러리를](#) 참조하십시오.

## ITSM

[IT 서비스 관리를](#) 참조하십시오.

## L

### 레이블 기반 액세스 제어(LBAC)

사용자 및 데이터 자체에 각각 보안 레이블 값을 명시적으로 할당하는 필수 액세스 제어(MAC)를 구현한 것입니다. 사용자 보안 레이블과 데이터 보안 레이블 간의 교차 부분에 따라 사용자가 볼 수 있는 행과 열이 결정됩니다.

### 랜딩 존

랜딩 존은 확장성과 안전성을 갖춘 잘 설계된 다중 계정 AWS 환경입니다. 조직은 여기에서부터 보안 및 인프라 환경에 대한 확신을 가지고 워크로드와 애플리케이션을 신속하게 시작하고 배포할 수 있습니다. 랜딩 존에 대한 자세한 내용은 [Setting up a secure and scalable multi-account AWS environment](#)를 참조하세요.

### 대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

## LBAC

[레이블 기반 액세스 제어를](#) 참조하십시오.

### 최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 [최소 권한 적용](#)을 참조하세요.

### 리프트 앤드 시프트

[7 R](#)을 참조하십시오.

## 리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. [엔디안도](#) 참조하십시오.

### 하위 환경

[환경 참조.](#)

## M

### 기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공지능의 한 유형입니다. ML은 사물 인터넷 (IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 [기계 학습](#)을 참조하세요.

### 기본 브랜치

[브랜치](#) 참조.

### 매니지드 서비스

AWS 서비스인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하며 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. 관리형 서비스의 예로는 아마존 심플 스토리지 서비스 (Amazon S3) 와 아마존 DynamoDB가 있습니다. 이러한 서비스를 추상화된 서비스라고도 합니다.

### MAP

[Migration Acceleration 프로그램](#)을 참조하십시오.

### 기구

도구를 만들고 도구 채택을 유도한 다음 결과를 검토하여 조정하는 전체 프로세스입니다. 메커니즘은 작동하면서 자체적으로 강화되고 개선되는 사이클입니다. 자세한 내용은 AWS Well-Architected [프레임워크에서의 메커니즘 구축](#)을 참조하십시오.

### 멤버 계정

AWS Organizations의 조직에 속하는 관리 계정 이외의 모든 AWS 계정입니다. 하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

### 마이크로서비스

잘 정의된 API를 통해 통신하고 일반적으로 소규모 자체 팀이 소유하는 소규모 독립 서비스입니다. 예를 들어, 보험 시스템에는 영업, 마케팅 등의 비즈니스 역량이나 구매, 청구, 분석 등의 하위 영역

에 매핑되는 마이크로 서비스가 포함될 수 있습니다. 마이크로서비스의 이점으로 민첩성, 유연한 확장, 손쉬운 배포, 재사용 가능한 코드, 복원력 등이 있습니다. 자세한 내용은 [AWS 서버리스 서비스를 사용하여 마이크로서비스 통합](#)을 참조하세요.

## 마이크로서비스 아키텍처

각 애플리케이션 프로세스를 마이크로서비스로 실행하는 독립 구성 요소를 사용하여 애플리케이션을 구축하는 접근 방식입니다. 이러한 마이크로서비스는 경량 API를 사용하여 잘 정의된 인터페이스를 통해 통신합니다. 애플리케이션의 특정 기능에 대한 수요에 맞게 이 아키텍처의 각 마이크로서비스를 업데이트, 배포 및 조정할 수 있습니다. 자세한 내용은 [AWS에서 마이크로서비스 구현](#)을 참조하세요.

## Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 마이그레이션 초기 비용을 상쇄할 수 있도록 컨설팅 지원, 교육 및 서비스를 제공하는 AWS 프로그램입니다. MAP에는 레거시 마이그레이션을 체계적인 방식으로 실행하기 위한 마이그레이션 방법론과 일반적인 마이그레이션 시나리오를 자동화하고 가속화하는 도구 세트가 포함되어 있습니다.

## 대규모 마이그레이션

애플리케이션 포트폴리오의 대다수를 웨이브를 통해 클라우드로 이동하는 프로세스로, 각 웨이브에서 더 많은 애플리케이션이 더 빠른 속도로 이동합니다. 이 단계에서는 이전 단계에서 배운 모범 사례와 교훈을 사용하여 팀, 도구 및 프로세스의 마이그레이션 팩토리를 구현하여 자동화 및 민첩한 제공을 통해 워크로드 마이그레이션을 간소화합니다. 이것은 [AWS 마이그레이션 전략](#)의 세 번째 단계입니다.

## 마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자, 스프린트에서 일하는 DevOps 전문가가 포함됩니다. 엔터프라이즈 애플리케이션 포트폴리오의 20~50%는 공장 접근 방식으로 최적화할 수 있는 반복되는 패턴으로 구성되어 있습니다. 자세한 내용은 이 콘텐츠 세트의 [클라우드 마이그레이션 팩토리 가이드](#)와 [마이그레이션 팩토리에 대한 설명](#)을 참조하세요.

## 마이그레이션 메타데이터

마이그레이션을 완료하는 데 필요한 애플리케이션 및 서버에 대한 정보 각 마이그레이션 패턴에는 서로 다른 마이그레이션 메타데이터 세트가 필요합니다. 마이그레이션 메타데이터의 예로는 대상 서브넷, 보안 그룹 및 AWS 계정이 있습니다.

## 마이그레이션 패턴

사용되는 마이그레이션 전략, 마이그레이션 대상, 마이그레이션 애플리케이션 또는 서비스를 자세히 설명하는 반복 가능한 마이그레이션 작업입니다. 예를 들어, AWS Application Migration Service를 사용하여 Amazon EC2로 마이그레이션을 리호스팅합니다.

### Migration Portfolio Assessment(MPA)

AWS 클라우드로 마이그레이션의 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다. MPA는 상세한 포트폴리오 평가(서버 적정 규모 조정, 가격 책정, TCO 비교, 마이그레이션 비용 분석)와 마이그레이션 계획(애플리케이션 데이터 분석 및 데이터 수집, 애플리케이션 그룹화, 마이그레이션 우선순위 지정, 웨이브 계획)을 제공합니다. [MPA 도구](#)(로그인 필요)는 모든 AWS 컨설턴트와 APN 파트너 컨설턴트에게 무료로 제공됩니다.

### 마이그레이션 준비 상태 평가(MRA)

AWS CAF를 사용하여 조직의 클라우드 준비 상태에 대한 인사이트를 얻고, 장단점을 파악하고, 파악된 격차를 해소하기 위한 실행 계획을 수립하는 프로세스입니다. 자세한 내용은 [마이그레이션 준비 가이드](#)를 참조하세요. MRA는 [AWS 마이그레이션 전략](#)의 첫 번째 단계입니다.

### 마이그레이션 전략

워크로드를 AWS 클라우드로 마이그레이션하는 데 사용되는 접근 방식입니다. 자세한 내용은 이 용어집의 [7R](#) 항목을 참조하고 대규모 마이그레이션을 [가속화하기 위한 조직 동원을](#) 참조하십시오.

### ML

[기계 학습을 참조하십시오.](#)

### MPA

[마이그레이션 포트폴리오 평가를](#) 참조하십시오.

### 현대화

비용을 절감하고 효율성을 높이고 혁신을 활용하기 위해 구식(레거시 또는 모놀리식) 애플리케이션과 해당 인프라를 클라우드의 민첩하고 탄력적이고 가용성이 높은 시스템으로 전환하는 것입니다. 자세한 내용은 [AWS 클라우드에서 애플리케이션 현대화 전략](#)을 참조하세요.

### 현대화 준비 상태 평가

조직 애플리케이션의 현대화 준비 상태를 파악하고, 이점, 위험 및 종속성을 식별하고, 조직이 해당 애플리케이션의 향후 상태를 얼마나 잘 지원할 수 있는지를 확인하는 데 도움이 되는 평가입니다. 평가 결과는 대상 아키텍처의 청사진, 현대화 프로세스의 개발 단계와 마일스톤을 자세히 설명하는



로드맵 및 파악된 격차를 해소하기 위한 실행 계획입니다. 자세한 내용은 [AWS 클라우드에서 애플리케이션의 현대화 준비 상태 평가](#)를 참조하세요.

### 모놀리식 애플리케이션(모놀리식 유형)

긴밀하게 연결된 프로세스를 사용하여 단일 서비스로 실행되는 애플리케이션입니다. 모놀리식 애플리케이션에는 몇 가지 단점이 있습니다. 한 애플리케이션 기능에 대한 수요가 급증하면 전체 아키텍처 규모를 조정해야 합니다. 코드 베이스가 커지면 모놀리식 애플리케이션의 기능을 추가하거나 개선하는 것도 더 복잡해집니다. 이러한 문제를 해결하기 위해 마이크로서비스 아키텍처를 사용할 수 있습니다. 자세한 내용은 [마이크로서비스로 모놀리식 유형 분해](#)를 참조하세요.

### 멀티클래스 분류

여러 클래스에 대한 예측(2개 이상의 결과 중 하나 예측)을 생성하는 데 도움이 되는 프로세스입니다. 예를 들어, ML 모델이 '이 제품은 책인가요, 자동차인가요, 휴대폰인가요?' 또는 '이 고객이 가장 관심을 갖는 제품 범주는 무엇인가요?'라고 물을 수 있습니다.

### 변경 가능한 인프라

프로덕션 워크로드를 위해 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 안정성 및 예측 가능성을 개선하기 위해 AWS Well-Architected Framework는 [변경 불가능한](#) 인프라를 모범 사례로 사용할 것을 권장합니다.

## O

### OAC

[원본 액세스 제어를 참조하십시오.](#)

### 좋아요

[원본 액세스 ID를 참조하십시오.](#)

### OCM

[조직 변경 관리를 참조하십시오.](#)

### 오프라인 마이그레이션

마이그레이션 프로세스 중 소스 워크로드가 중단되는 마이그레이션 방법입니다. 이 방법은 가동 중지 증가를 수반하며 일반적으로 작고 중요하지 않은 워크로드에 사용됩니다.

## 이

[운영 통합을 참조하십시오.](#)

안녕하세요.

[운영 수준 계약을](#) 참조하십시오.

## 온라인 마이그레이션

소스 워크로드를 오프라인 상태로 전환하지 않고 대상 시스템에 복사하는 마이그레이션 방법입니다. 워크로드에 연결된 애플리케이션은 마이그레이션 중에도 계속 작동할 수 있습니다. 이 방법은 가동 중지 차단 또는 최소화를 수반하며 일반적으로 중요한 프로덕션 워크로드에 사용됩니다.

## 운영 수준 협약(OLA)

서비스 수준에 관한 계약(SLA)을 지원하기 위해 직무 IT 그룹이 서로에게 제공하기로 약속한 내용을 명확히 하는 계약입니다.

## 운영 준비 상태 검토 (ORR)

인시던트 및 발생 가능한 실패의 범위를 이해, 평가, 예방 또는 줄이는 데 도움이 되는 질문 및 관련 모범 사례로 구성된 체크리스트입니다. 자세한 내용은 Well-Architected AWS 프레임워크의 [운영 준비 상태 검토 \(ORR\)](#) 를 참조하십시오.

## 운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 [운영 통합 가이드](#)를 참조하세요.

## 조직 트레일

AWS Organizations의 조직 내 모든 AWS 계정에 대한 모든 이벤트를 로깅하기 위해 AWS CloudTrail에서 생성하는 트레일입니다. 이 트레일은 조직에 속한 각 AWS 계정에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 설명서의 [조직을 위한 트레일 만들기를](#) 참조하십시오.

CloudTrail

## 조직 변경 관리(OCM)

사람, 문화 및 리더십 관점에서 중대하고 파괴적인 비즈니스 혁신을 관리하기 위한 프레임워크입니다. OCM은 변화 채택을 가속화하고, 과도기적 문제를 해결하고, 문화 및 조직적 변화를 주도함으로써 조직이 새로운 시스템 및 전략을 준비하고 전환할 수 있도록 지원합니다. AWS 마이그레이션 전략에서는 클라우드 채택 프로젝트에 필요한 변화 속도 때문에 이 프레임워크를 인력 가속화라고 합니다. 자세한 내용은 [사용 가이드](#)를 참조하세요.

## 오리진 액세스 제어(OAC)

CloudFront에서는 Amazon Simple Storage Service (Amazon S3) 콘텐츠의 보안을 위해 액세스를 제한하는 향상된 옵션을 제공합니다. OAC는 모든 AWS 리전의 모든 S3 버킷, AWS KMS(SSE-KMS)를 사용한 서버측 암호화, S3 버킷에 대한 동적 PUT 및 DELETE 요청을 지원합니다.

## 오리진 액세스 ID(OAI)

CloudFront에서는 Amazon S3 콘텐츠 보안을 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 Amazon S3가 인증할 수 있는 보안 주체를 CloudFront 생성합니다. 인증된 보안 주체는 특정 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. CloudFront 더 세분화되고 향상된 액세스 제어를 제공하는 [OAC](#)도 참조하세요.

또는

[운영 준비 상태](#) 검토를 참조하십시오.

## 아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작되는 네트워크 연결을 처리하는 VPC입니다. [AWS Security Reference Architecture](#)에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

## P

### 권한 경계

사용자나 역할이 가질 수 있는 최대 권한을 설정하기 위해 IAM 보안 주체에 연결되는 IAM 관리 정책입니다. 자세한 내용은 IAM 설명서의 [권한 경계](#)를 참조하세요.

### 개인 식별 정보(PII)

직접 보거나 다른 관련 데이터와 함께 짝을 지을 때 개인의 신원을 합리적으로 추론하는 데 사용할 수 있는 정보입니다. PII의 예로는 이름, 주소, 연락처 정보 등이 있습니다.

### PII

[개인 식별 정보를](#) 참조하십시오.

### 플레이북

클라우드에서 핵심 운영 기능을 제공하는 등 마이그레이션과 관련된 작업을 캡처하는 일련의 사전 정의된 단계입니다. 플레이북은 스크립트, 자동화된 런북 또는 현대화된 환경을 운영하는 데 필요한 프로세스나 단계 요약의 형태를 취할 수 있습니다.

### 정책

[권한을 정의 \(ID 기반 정책 참조\)](#) 하거나, [액세스 조건을 지정 \(리소스 기반 정책 참조\)](#) 하거나, [조직의 모든 계정에 대한 최대 권한을 정의 AWS Organizations \(서비스 제어 정책 참조\)](#) 할 수 있는 [개체입니다](#).

## 다국어 지속성

데이터 액세스 패턴 및 기타 요구 사항을 기반으로 독립적으로 마이크로서비스의 데이터 스토리지 기술 선택. 마이크로서비스가 동일한 데이터 스토리지 기술을 사용하는 경우 구현 문제가 발생하거나 성능이 저하될 수 있습니다. 요구 사항에 가장 적합한 데이터 스토어를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다. 자세한 내용은 [마이크로서비스에서 데이터 지속성 활성화](#)를 참조하세요.

## 포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 [마이그레이션 준비 상태 평가](#)를 참조하세요.

## 조건자

일반적으로 조항에 있는 true false OR를 반환하는 쿼리 조건입니다. WHERE

## 조건부 푸시다운

전송하기 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄어들고 쿼리 성능이 향상됩니다.

## 예방적 제어

이벤트 발생을 방지하도록 설계된 보안 제어입니다. 이 제어는 네트워크에 대한 무단 액세스나 원치 않는 변경을 방지하는 데 도움이 되는 1차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 [Preventative controls](#)를 참조하세요.

## 보안 주체

작업을 수행하고 리소스에 액세스할 수 있는 AWS의 객체입니다. 이 엔터티는 일반적으로 AWS 계정의 루트 사용자, IAM 역할 또는 사용자입니다. 자세한 내용은 IAM 설명서의 [역할 용어 및 개념](#)의 보안 주체를 참조하세요.

## 개인 정보 보호 중심 설계

전체 엔지니어링 프로세스에서 개인 정보를 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

## 프라이빗 호스팅 영역

Amazon Route 53에서 하나 이상의 VPC 내 도메인과 하위 도메인에 대한 DNS 쿼리에 응답하는 방법에 대한 정보가 담긴 컨테이너입니다. 자세한 내용은 Route 53 설명서의 [프라이빗 호스팅 영역 작업](#)을 참조하세요.

## 사전 예방적 제어

규정을 준수하지 않는 리소스의 배포를 방지하도록 설계된 [보안 제어입니다](#). 이러한 컨트롤은 리소스를 프로비저닝하기 전에 리소스를 스캔합니다. 리소스가 컨트롤과 호환되지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 [컨트롤 참조 안내서](#)를 참조하고 보안 제어 구현의 [사전 제어를](#) 참조하십시오. AWS

## 프로덕션 환경

[환경을](#) 참조하십시오.

## 가명화

데이터세트의 개인 식별자를 자리 표시자 값으로 바꾸는 프로세스입니다. 가명화는 개인 정보를 보호하는 데 도움이 될 수 있습니다. 가명화된 데이터는 여전히 개인 데이터로 간주됩니다.

## Q

### 쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 일련의 단계 (예: 지침).

### 쿼리 계획 회귀

데이터베이스 서비스 최적화 프로그램이 데이터베이스 환경을 변경하기 전보다 덜 최적의 계획을 선택하는 경우입니다. 통계, 제한 사항, 환경 설정, 쿼리 파라미터 바인딩 및 데이터베이스 엔진 업데이트의 변경으로 인해 발생할 수 있습니다.

## R

### RACI 매트릭스

RACI ([책임](#), [책임](#), [상담](#), [정보 제공](#)) 을 참조하십시오.

### 랜섬웨어

결제 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다.

### RASCI 매트릭스

[책임](#), [책임](#), [상담](#), [정보 제공 \(RACI\)](#) 을 참조하십시오.

## RCAC

[행 및 열 액세스 제어를](#) 참조하십시오.

### 읽기 전용 복제본

읽기 전용 용도로 사용되는 데이터베이스의 사본입니다. 쿼리를 읽기 전용 복제본으로 라우팅하여 기본 데이터베이스의 로드를 줄일 수 있습니다.

### 재설계

[7 R을](#) 참조하십시오.

### Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 시점 사이에 허용 가능한 데이터 손실이 결정됩니다.

### Recovery Time Objective(RTO)

서비스 중단과 서비스 복구 사이에 허용되는 최대 지연 시간입니다.

### 리팩터링

[7 R을](#) 참조하십시오.

### 리전

AWS 리소스를 지리적 영역에 모아 놓은 것입니다. 각 AWS 리전은 내결함성, 안정성 및 복원력을 제공하기 위해 격리되어 있으며 다른 리전과는 독립적입니다. 자세한 내용은 AWS 일반 참조의 [AWS 리전 관리](#)를 참조하세요.

### 회귀

숫자 값을 예측하는 ML 기법입니다. 예를 들어, '이 집은 얼마에 팔릴까?'라는 문제를 풀기 위해 ML 모델은 선형 회귀 모델을 사용하여 주택에 대해 알려진 사실(예: 면적)을 기반으로 주택의 매매 가격을 예측할 수 있습니다.

### 리호스팅

[7 R을](#) 참조하십시오.

### release

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

### 고쳐 놓다

[7 R을](#) 참조하십시오.

## 리플랫폼

[7 R](#)을 참조하십시오.

### 환매

[7 R](#)을 참조하십시오.

### 리소스 기반 정책

Amazon S3 버킷, 엔드포인트, 암호화 키 등의 리소스에 연결된 정책입니다. 이 유형의 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

### RACI(Responsible, Accountable, Consulted, Informed) 매트릭스

마이그레이션 활동 및 클라우드 운영에 참여하는 모든 당사자의 역할과 책임을 정의하는 매트릭스입니다. 매트릭스 이름은 매트릭스에 정의된 책임 유형에서 파생됩니다: 실무 담당자 (R), 의사 결정권자 (A), 업무 수행 조연자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원자를 포함하면 매트릭스를 RASCI 매트릭스라고 하고, 지원자를 제외하면 RACI 매트릭스라고 합니다.

### 대응 제어

보안 기준에서 벗어나거나 부정적인 이벤트를 해결하도록 설계된 보안 제어입니다. 자세한 내용은 Implementing security controls on AWS의 [Responsive controls](#)를 참조하세요.

### retain

[7 R](#)을 참조하십시오.

### 은퇴

[7 R](#)을 참조하십시오.

### 회전

공격자가 자격 증명에 액세스하는 것을 더 어렵게 만들기 위해 [암호](#)를 주기적으로 업데이트하는 프로세스입니다.

### 행 및 열 액세스 제어(RCAC)

액세스 규칙이 정의된 기본적이고 유연한 SQL 표현식을 사용합니다. RCAC는 행 권한과 열 마스크로 구성됩니다.

### RPO

[복구 지점 목표를](#) 참조하십시오.

### RPO

[복구 시간 목표를](#) 참조하십시오.

## 런북

특정 작업을 수행하는 데 필요한 일련의 수동 또는 자동 절차입니다. 일반적으로 오류율이 높은 반복 작업이나 절차를 간소화하기 위해 런북을 만듭니다.

## S

### SAML 2.0

많은 ID 제공업체 (IdPs) 가 사용하는 개방형 표준입니다. 이 기능은 페더레이션형 AWS Single Sign-On(SSO)을 활성화하므로 조직의 모든 멤버에 대해 IAM 사용자를 생성하지 않아도 사용자가 AWS Management Console에 로그인하거나 AWS API 작업을 직접적으로 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 [SAML 2.0 기반 페더레이션 정보](#)를 참조하세요.

### SCP

[서비스 제어 정책을](#) 참조하십시오.

### secret

에는 AWS Secrets Manager 암호화된 형태로 저장하는 비밀번호나 사용자 자격 증명과 같은 기밀 또는 제한된 정보. 비밀 값과 해당 메타데이터로 구성됩니다. 비밀 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 Secrets Manager 문서의 [시크릿](#)을 참조하십시오.

### 보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. [보안 제어에는 예방적, 탐정적, 대응적, 사전 예방적 등 네 가지 기본 유형이 있습니다.](#)

### 보안 강화

공격 표면을 줄여 공격에 대한 저항력을 높이는 프로세스입니다. 더 이상 필요하지 않은 리소스 제거, 최소 권한 부여의 보안 모범 사례 구현, 구성 파일의 불필요한 기능 비활성화 등의 작업이 여기에 포함될 수 있습니다.

### 보안 정보 및 이벤트 관리(SIEM) 시스템

보안 정보 관리(SIM)와 보안 이벤트 관리(SEM) 시스템을 결합하는 도구 및 서비스입니다. SIEM 시스템은 서버, 네트워크, 디바이스 및 기타 소스에서 데이터를 수집, 모니터링 및 분석하여 위협과 보안 침해를 탐지하고 알림을 생성합니다.



## 보안 대응 자동화

보안 이벤트에 자동으로 대응하거나 보안 이벤트를 해결하도록 설계된 사전 정의되고 프로그래밍된 조치입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 [탐지](#) 또는 [대응형](#) 보안 제어 역할을 합니다. AWS 자동 응답 조치의 예로는 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치, 자격 증명 교체 등이 있습니다.

## 서버측 암호화

데이터를 수신하는 AWS 서비스가 대상에서 데이터를 암호화하는 것입니다.

## 서비스 제어 정책(SCP)

AWS Organizations에 속한 조직의 모든 계정에 대한 권한을 중앙 집중식으로 제어하는 정책입니다. SCP는 관리자가 사용자 또는 역할에 위임할 수 있는 작업에 대해 제한을 설정하거나 가드레일을 정의합니다. SCP를 허용 목록 또는 거부 목록으로 사용하여 허용하거나 금지할 서비스 또는 작업을 지정할 수 있습니다. 자세한 내용은 AWS Organizations 설명서의 [서비스 제어 정책](#)을 참조하세요.

## 서비스 엔드포인트

AWS 서비스에 대한 진입점의 URL입니다. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 [AWS 서비스 엔드포인트](#)를 참조하세요.

## 서비스 수준에 관한 계약(SLA)

IT 팀이 고객에게 제공하기로 약속한 내용(예: 서비스 가동 시간 및 성능)을 명시한 계약입니다.

## 서비스 수준 지표 (SLI)

오류율, 가용성 또는 처리량과 같은 서비스의 성능 측면을 측정하는 것입니다.

## 서비스 수준 목표 (SLO)

[서비스 수준 지표로 측정되는 서비스 상태를 나타내는 대상 지표입니다.](#)

## 공동 책임 모델

클라우드 보안 및 규정 준수를 위해 AWS와 공유하는 책임을 설명하는 모델입니다. AWS는 클라우드의 보안을 담당하고, 사용자는 클라우드에서 보안을 담당합니다. 자세한 내용은 [공동 책임 모델](#)을 참조하세요.

## 시앰

[보안 정보 및 이벤트 관리 시스템](#)을 참조하십시오.

## 단일 장애 지점 (SPOF)

응용 프로그램의 중요한 단일 구성 요소에서 발생한 오류로 인해 시스템이 중단될 수 있습니다.

### SLA

SLA ([서비스 수준 계약](#)) 를 참조하십시오.

### SLI

[서비스 수준](#) 표시기를 참조하십시오.

### SLO

[서비스 수준 목표를](#) 참조하십시오.

### split-and-seed 모델

현대화 프로젝트를 확장하고 가속화하기 위한 패턴입니다. 새로운 기능과 제품 릴리스가 정의되면 핵심 팀이 분할되어 새로운 제품 팀이 만들어집니다. 이를 통해 조직의 역량과 서비스 규모를 조정하고, 개발자 생산성을 개선하고, 신속한 혁신을 지원할 수 있습니다. 자세한 내용은 의 [애플리케이션 현대화를 위한 단계별 접근 방식을 참조하십시오. AWS 클라우드](#)

### SPOF

[단일 장애 지점](#) 보기

### 스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정 데이터를 저장하고 하나 이상의 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 구성 구조입니다. 이 구조는 [데이터 웨어하우스에서](#) 사용하거나 비즈니스 인텔리전스 용도로 설계되었습니다.

### Strangler Fig 패턴

레거시 시스템을 폐기할 수 있을 때까지 시스템 기능을 점진적으로 다시 작성하고 교체하여 모놀리식 시스템을 현대화하기 위한 접근 방식. 이 패턴은 무화과 덩굴이 나무로 자라 결국 숙주를 압도하고 대체하는 것과 비슷합니다. [Martin Fowler](#)가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 [컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET\(ASMX\) 웹 서비스를 점진적으로 현대화하는 방법](#)을 참조하세요.

### 서브넷

VPC의 IP 주소 범위입니다. 서브넷은 단일 가용 영역에 상주해야 합니다.

## 대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

## 합성 테스트

잠재적 문제를 감지하거나 성능을 모니터링하기 위해 사용자 상호 작용을 시뮬레이션하는 방식으로 시스템을 테스트합니다. [Amazon CloudWatch Synthetics](#)를 사용하여 이러한 테스트를 생성할 수 있습니다.

# T

## tags

AWS 리소스를 구성하는 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색 및 필터링할 수 있습니다. 자세한 내용은 [AWS 리소스에 태그 지정](#)을 참조하십시오.

## 대상 변수

지도 ML에서 예측하려는 값으로, 결과 변수라고도 합니다. 예를 들어, 제조 설정에서 대상 변수는 제품 결함일 수 있습니다.

## 작업 목록

런북을 통해 진행 상황을 추적하는 데 사용되는 도구입니다. 작업 목록에는 런북의 개요와 완료해야 할 일반 작업 목록이 포함되어 있습니다. 각 일반 작업에 대한 예상 소요 시간, 소유자 및 진행 상황이 작업 목록에 포함됩니다.

## 테스트 환경

[환경을 참조하십시오.](#)

## 훈련

ML 모델이 학습할 수 있는 데이터를 제공하는 것입니다. 훈련 데이터에는 정답이 포함되어야 합니다. 학습 알고리즘은 훈련 데이터에서 대상(예측하려는 답)에 입력 데이터 속성을 매핑하는 패턴을 찾고, 이러한 패턴을 캡처하는 ML 모델을 출력합니다. 그런 다음 ML 모델을 사용하여 대상을 모르는 새 데이터에 대한 예측을 할 수 있습니다.

## 전송 게이트웨이

VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 [Transit Gateway란 무엇입니까?](#) 섹션을 참조하세요.

## 트렁크 기반 워크플로

개발자가 기능 브랜치에서 로컬로 기능을 구축하고 테스트한 다음 해당 변경 사항을 기본 브랜치에 병합하는 접근 방식입니다. 이후 기본 브랜치는 개발, 프로덕션 이전 및 프로덕션 환경에 순차적으로 구축됩니다.

### 신뢰할 수 있는 액세스

사용자를 대신하여 AWS Organizations의 조직과 해당 계정에서 작업을 수행하도록 지정하는 서비스에 권한을 부여하는 것입니다. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관리 작업을 수행합니다. 자세한 내용은 AWS Organizations 설명서의 [다른 AWS 서비스와 함께 AWS Organizations 사용](#)을 참조하세요.

### 튜닝

ML 모델의 정확도를 높이기 위해 훈련 프로세스의 측면을 여러 변경하는 것입니다. 예를 들어, 레이블링 세트를 생성하고 레이블을 추가한 다음 다양한 설정에서 이러한 단계를 여러 번 반복하여 모델을 최적화하는 방식으로 ML 모델을 훈련할 수 있습니다.

### 피자 두 판 팀

피자 두 판이면 먹을 수 있는 소규모 DevOps 팀이죠. 피자 두 판 팀 규모는 소프트웨어 개발에 있어 가능한 최상의 공동 작업 기회를 보장합니다.

## U

### 불확실성

예측 ML 모델의 신뢰성을 저해할 수 있는 부정확하거나 불완전하거나 알려지지 않은 정보를 나타내는 개념입니다. 불확실성에는 두 가지 유형이 있습니다. 인식론적 불확실성은 제한적이고 불완전한 데이터에 의해 발생하는 반면, 우연한 불확실성은 데이터에 내재된 노이즈와 무작위성에 의해 발생합니다. 자세한 내용은 [Quantifying uncertainty in deep learning systems](#) 가이드를 참조하세요.

### 차별화되지 않은 작업

애플리케이션을 만들고 운영하는 데 필요하지만 최종 사용자에게 직접적인 가치를 제공하거나 경쟁 우위를 제공하지 못하는 작업을 헤비 리프팅이라고도 합니다. 차별화되지 않은 작업의 예로는 조달, 유지보수, 용량 계획 등이 있습니다.

### 상위 환경

[환경을](#) 보세요.

## V

### 정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수반하는 데이터베이스 유지 관리 작업입니다.

### 버전 제어

리포지토리의 소스 코드 변경과 같은 변경 사항을 추적하는 프로세스 및 도구입니다.

### VPC 피어링

프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 있게 하는 두 VPC 간의 연결입니다. 자세한 내용은 Amazon VPC 설명서의 [VPC 피어링이란?](#)을 참조하세요.

### 취약성

시스템 보안을 손상시키는 소프트웨어 또는 하드웨어 결함입니다.

## W

### 웜 캐시

자주 액세스하는 최신 관련 데이터를 포함하는 버퍼 캐시입니다. 버퍼 캐시에서 데이터베이스 인스턴스를 읽을 수 있기 때문에 주 메모리나 디스크에서 읽는 것보다 빠릅니다.

### 웜 데이터

자주 액세스하지 않는 데이터입니다. 이런 종류의 데이터를 쿼리할 때는 일반적으로 적절히 느린 쿼리가 허용됩니다.

### 윈도우 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에 대해 계산을 수행하는 SQL 함수입니다. 윈도우 함수는 이동 평균을 계산하거나 현재 행의 상대적 위치를 기반으로 행 값에 액세스하는 등의 작업을 처리하는 데 유용합니다.

### 워크로드

고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음입니다.

## 워크스트림

마이그레이션 프로젝트에서 특정 작업 세트를 담당하는 직무 그룹입니다. 각 워크스트림은 독립적이지만 프로젝트의 다른 워크스트림을 지원합니다. 예를 들어, 포트폴리오 워크스트림은 애플리케이션 우선순위 지정, 웨이브 계획, 마이그레이션 메타데이터 수집을 담당합니다. 포트폴리오 워크스트림은 이러한 자산을 마이그레이션 워크스트림에 전달하고, 마이그레이션 워크스트림은 서버와 애플리케이션을 마이그레이션합니다.

## 원

[한 번 쓰고, 많이 읽으세요.](#)

## WQF

[AWS 워크로드 검증 프레임워크](#)를 참조하십시오.

### 한 번 작성하고 여러 번 읽기 (WORM)

데이터를 한 번 쓰고 데이터가 삭제되거나 수정되지 않도록 하는 스토리지 모델입니다. 인증된 사용자는 필요한 만큼 데이터를 여러 번 읽을 수 있지만 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 [변경할 수 없는](#) 것으로 간주됩니다.

## Z

### 제로데이 익스플로잇

[제로데이](#) 취약점을 악용하는 공격 (일반적으로 멀웨어)입니다.

### 제로데이 취약성

프로덕션 시스템의 명백한 결함 또는 취약성입니다. 위협 행위자는 이러한 유형의 취약성을 사용하여 시스템을 공격할 수 있습니다. 개발자는 공격의 결과로 취약성을 인지하는 경우가 많습니다.

### 좀비 애플리케이션

평균 CPU 및 메모리 사용량이 5% 미만인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하는 것이 일반적입니다.

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