에서 봇 제어 전략 구현 AWS

AWS 권장 가이드

AWS 권장 가이드: 에서 봇 제어 전략 구현 AWS

Table of Contents

에 봇 제어 전략 구현 AWS

Amazon Web Services (기고자)

2024년 2월 (문서 기록)

우리가 알고 있는 것처럼 인터넷은 봇이 없었다면 불가능했을 것입니다. 봇은 인터넷을 통해 자동화된 작업을 실행하고 인간의 활동이나 상호 작용을 시뮬레이션합니다. 이를 통해 기업은 프로세스와 작업의 효율성을 높일 수 있습니다. 웹 크롤러와 같은 유용한 봇은 인터넷에서 정보를 인덱싱하여 검색 쿼리와 가장 관련성이 높은 정보를 빠르게 찾을 수 있도록 도와줍니다. 봇은 비즈니스를 개선하고 기업에 가치를 제공하는 좋은 메커니즘입니다. 그러나 시간이 지나면서 악의적인 행위자들은 새롭고 창의적인 방식으로 기존 시스템과 애플리케이션을 악용하는 수단으로 봇을 사용하기 시작했습니다.

봇넷은 봇과 그 영향을 확장하는 가장 잘 알려진 메커니즘입니다. 봇넷은 멀웨어에 감염되어 봇 허더 또는 봇 운영자로 알려진 단일 당사자의 통제 하에 있는 봇 네트워크입니다. 운영자는 하나의 중앙 지점에서 봇넷의 모든 컴퓨터에 동시에 조정된 작업을 수행하도록 명령할 수 있습니다. 이것이 봇넷을 (C2) 시스템이라고도 하는 이유입니다. command-and-control

봇넷의 규모는 수백만 개의 봇이 될 수 있습니다. 봇넷은 운영자가 대규모 작업을 수행할 수 있도록 도와줍니다. 봇넷은 원격 운영자의 제어 하에 있기 때문에 감염된 시스템은 업데이트를 수신하고 즉시 동작을 변경할 수 있습니다. 따라서 C2 시스템은 암시장에 있는 자사 봇넷 세그먼트에 대한 액세스 권한을 대여하여 상당한 금전적 이득을 얻을 수 있습니다.

봇넷의 보급률은 계속 증가하고 있습니다. 전문가들은 이를 악의적인 공격자들이 가장 선호하는 도구로 간주합니다. Mirai는 가장 규모가 큰 봇넷 중 하나입니다. 2016년에 등장하여 여전히 작동 중이며 최대 35만 대의 사물 인터넷 (IoT) 장치를 감염시킨 것으로 추정됩니다. 이 봇넷은 DDoS (분산 서비스 거부) 공격을 비롯한 다양한 유형의 활동에 맞게 조정되어 사용되었습니다. 최근에는 악의적인 공격자들이 주거용 프록시 서비스를 사용하여 IP 주소를 획득하여 활동을 더욱 난독화하고 트래픽을 수집하려고 했습니다. 이로 인해 합법적이고 상호 연결된 peer-to-peer 시스템이 구축되어 활동이 정교해지고 탐지 및 완화가 더욱 어려워집니다.

이 문서에서는 봇 환경, 애플리케이션에 미치는 영향, 사용 가능한 전략 및 방어 옵션에 중점을 둡니다. 이 규범적 지침과 모범 사례는 다양한 유형의 봇 공격을 이해하고 완화하는 데 도움이 됩니다. 또한 이 가이드에서는 봇 방어 전략을 지원하는 기능 AWS 서비스 및 각 전략이 애플리케이션을 보호하는 데 어떤 도움을 줄 수 있는지 설명합니다. 또한 봇 모니터링에 대한 개요와 솔루션 비용 최적화를 위한 모범 사례도 포함되어 있습니다.

봇 위협 및 작업 이해

Security Today에 따르면 인터넷상의 모든 트래픽 중 47% 이상이 봇 때문입니다. 여기에는 봇의 유용한 부분, 즉 자기 식별하고 가치를 제공하는 부분이 포함됩니다. 봇 트래픽의 약 30%는 DDoS 공격, 티켓 스캘링, 인벤토리 스크레이핑 또는 저장과 같은 악의적인 활동을 수행하는 식별되지 않은 봇입니다. Security™는 2023년 상반기 동안 볼륨 측정 DDoS 이벤트가 300% 증가했다고 보고합니다. 따라서이 주제가 더 관련성이 높아지고 사용 가능한 예방 및 보호 도구와 기술에 대한 지식이 더욱 중요해집니다.

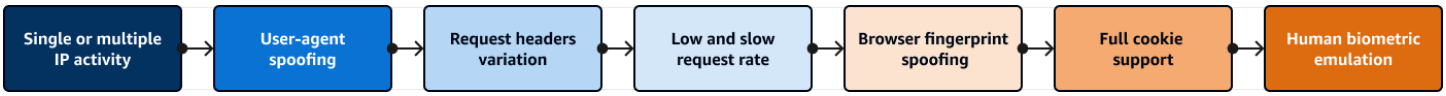
다음 표에서는 다양한 유형의 봇 활동과 각 봇이 미칠 수 있는 비즈니스 영향을 분류합니다. 이는 광범위한 목록이 아니며 가장 일반적인 봇 활동을 요약한 것입니다. 모니터링 및 완화 제어의 중요성을 강조합니다. 봇 위협의 광범위한 목록은 OWASP 애플리케이션에 대한 자동 위협 핸드북(OWASP 웹 사이트)을 참조하세요.

봇 활동 유형	설명	잠재적 영향
콘텐츠 스크레이핑	타사 사이트에서 사용할 독점 콘텐츠 복사	콘텐츠 복제, 브랜드 영향 및 공격적인 스크레이퍼로 인한 성능 문제로 인해 SEO에 미치는 영향
자격 증명 스터핑	웹 사이트에서 도난된 자격 증명 데이터베이스를 테스트하여 액세스 권한을 얻거나 정보를 검증합니다.	사기 및 계정 잠금과 같이 지원 쿼리를 늘리고 브랜드 신뢰를 떨어뜨리는 사용자의 문제
카드 균열	도난된 신용 카드 데이터의 데이터베이스를 테스트하여 누락된 정보를 검증하거나 보완합니다.	자격 증명 도용 및 사기, 사기 점수 손상과 같은 사용자의 문제
서비스 거부 공격	응답을 늦추거나 합법적인 트래픽에 사용할 수 없도록 하기 위해 특정 웹 사이트로의 트래픽 증가	수익 손실 및 평판 손상

봇 활동 유형	설명	잠재적 영향
계정 생성	오용 또는 재정적 이득을 목적으로 여러 계정 생성	성장 방해 및 마케팅 분석 왜곡
크기 조정	실제 소비자를 통해 한정된 가용성의 상품, 자주 사용하는 티켓 확보	판매 중인 상품에 대한 액세스 권한 부족과 같은 사용자의 수익 손실 및 문제

봇넷 작동 방식

봇넷 운영자의 전술, 기법 및 절차(TTP)는 시간이 지남에 따라 크게 발전했습니다. 회사에서 개발한 탐지 및 완화 기술을 따라잡아야 했습니다. 다음 그림은 이러한 변화를 보여줍니다. Botnet은 단순히 IP 주소를 운영 수단으로 사용하여 시작되었으며 결국 정교한 인간 생체 인식 에뮬레이션을 사용하도록 발전했습니다. 이러한 정교함은 비용이 많이 들고 모든 봇넷이 최첨단 도구를 사용하는 것은 아닙니다. 인터넷에는 운영자가 혼합되어 있으며, 작업에 가장 적합한 도구를 평가하여 투자 수익률을 높일 수 있습니다. 봇 방어의 한 가지 목표는 대상이 더 이상 실행 가능하지 않도록 봇넷 활동을 비용이 많이 드는 것으로 만드는 것입니다.



일반적으로 봇은 공통 또는 대상으로 분류됩니다.

- 일반 봇 - 이러한 봇은 자체 식별되며 브라우저 에뮬레이션을 시도하지 않습니다. 이러한 봇 중 다수는 콘텐츠 크롤링, 검색 엔진 최적화(SEO) 또는 집계와 같은 유용한 작업을 수행합니다. 이러한 일반적인 봇 중 어떤 봇이 사이트에 들어오는지, 트래픽 및 성능에 미치는 영향을 식별하고 이해하는 것이 중요합니다.
- 대상 봇 - 이러한 봇은 브라우저를 에뮬레이션하여 탐지를 회피하려고 합니다. 헤드리스 브라우저와 같은 브라우저 기술을 사용하거나 가짜 브라우저 지문을 사용합니다. JavaScript를 실행하고 쿠키를 지원할 수 있습니다. 의도가 항상 명확하지는 않으며 생성되는 트래픽이 일반 사용자 트래픽처럼 보일 수 있습니다.

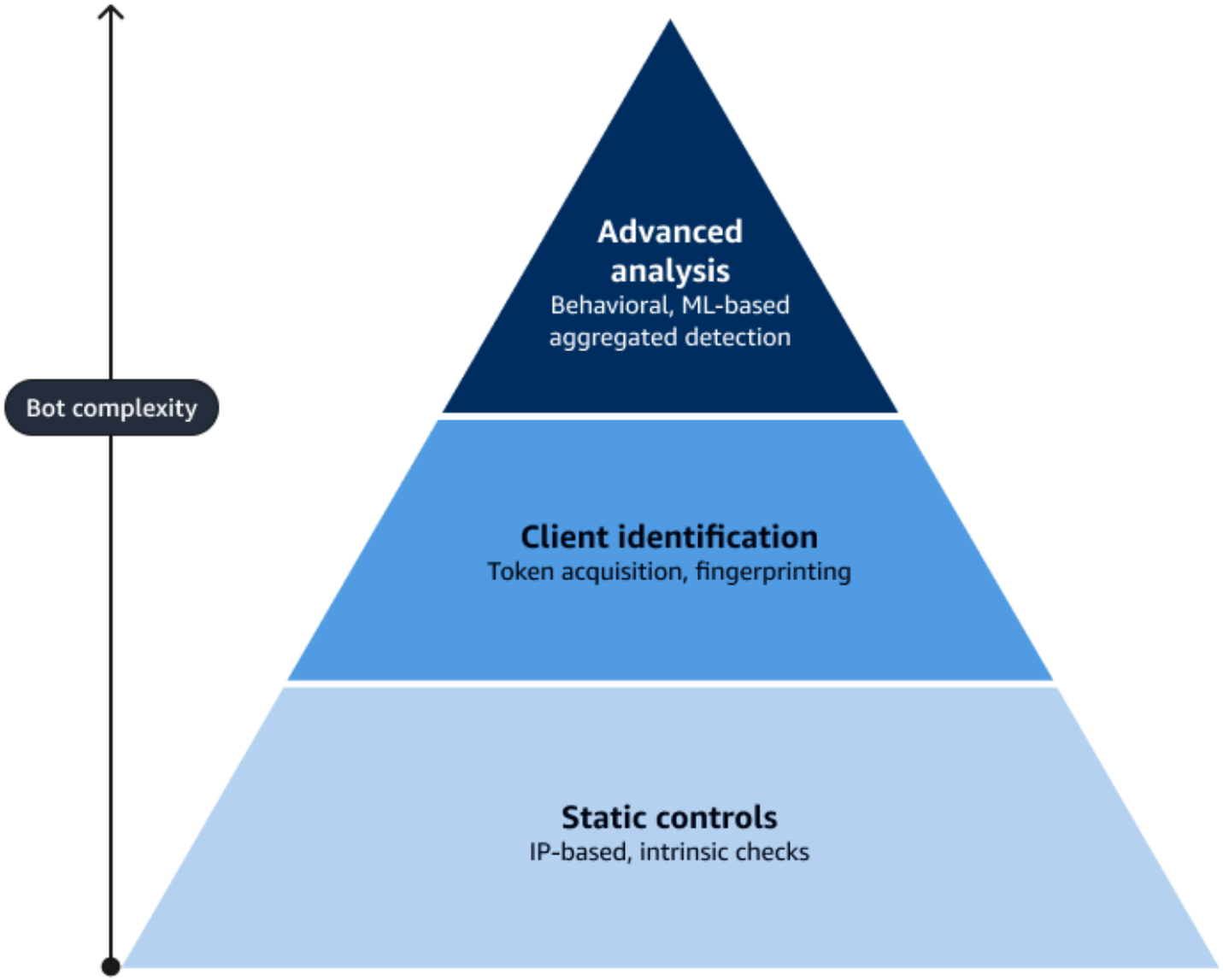
가장 고급이고 지속적인 대상 봇은 웹 사이트에서 인간과 유사한 마우스 움직임과 클릭을 생성하여 사람의 행동을 에뮬레이션합니다. 가장 정교하고 감지하기 어렵지만 운영 비용이 가장 많이 듭니다.

연산자는 이러한 기술을 결합하는 경우가 많습니다. 이렇게 하면 운영자의 최신 기술에 적응하기 위해 보호 및 완화 접근 방식을 자주 변경해야 하는 지속적인 추구 게임이 생성됩니다. 이러한 봇은 지능형 지속적 위협(APT)으로 간주됩니다. 자세한 내용은 NIST 리소스 센터의 고급 영구 위협을 참조하세요.

봇 제어 기법

봇 완화의 주요 목표는 자동화된 봇 활동이 조직의 웹 사이트, 서비스 및 애플리케이션에 미치는 부정적인 영향을 제한하는 것입니다. 사용되는 기술과 기법은 방어하려는 트래픽 또는 활동의 유형에 따라 다릅니다. 이를 위해서는 애플리케이션과 트래픽을 이해하는 것이 중요합니다. 시작할 위치에 대한 자세한 내용은이 가이드의 봇 제어 전략 모니터링 지침 섹션을 참조하세요.

일반적으로 봇 완화 솔루션이 제공하는 제어는 정적, 클라이언트 식별 및 고급 분석과 같은 상위 수준 범주로 그룹화할 수 있습니다. 다음 그림은 사용 가능한 다양한 기법과 봇 활동 복잡성에 따라 사용할 수 있는 방법을 보여줍니다. 이는 허용 목록 및 내장 검사와 같은 정적 제어를 사용하여 기본 또는 가장 광범위한 완화를 얻을 수 있는 방법을 강조합니다. 봇의 가장 작은 부분은 항상 가장 고급이며 이러한 봇을 완화하려면 고급 기술과 제어 조합이 필요합니다.



다음으로이 가이드에서는 각 범주와 해당 기술을 살펴봅니다. 또한에서 이러한 제어를 구현하는 AWS WAF 데 사용할 수 있는 옵션에 대해서도 설명합니다.

- 봇 관리를 위한 정적 제어
- 봇 관리를 위한 클라이언트 식별 제어
- 봇 관리를 위한 고급 분석 제어

봇 관리를 위한 정적 제어

작업을 수행하기 위해 정적 제어는 IP 주소 또는 헤더와 같은 HTTP(S) 요청의 정적 정보를 평가합니다. 이러한 제어는 세분화가 낮은 잘못된 봇 활동이나 확인 및 관리가 필요한 유용한 예상 봇 트래픽에 유용할 수 있습니다. 정적 제어 기법에는 허용 목록, IP 기반 제어 및 내장 검사가 포함됩니다.

목록 허용

허용 목록은 기존 봇 완화 제어를 통해 식별된 친숙한 트래픽을 허용하는 제어입니다. 이를 수행하는 방법에는 여러 가지가 있습니다. 가장 간단한 방법은 IP 주소 집합 또는 유사한 일치 조건과 일치하는 규칙을 사용하는 것입니다. 요청이 `Allow` 작업으로 설정된 규칙과 일치하면 후속 규칙에 의해 평가되지 않습니다. 경우에 따라 특정 규칙만 실행되지 않도록 해야 합니다. 즉, 모든 규칙이 아닌 한 규칙에 대한 목록을 허용해야 합니다. 이는 규칙에 대한 거짓 긍정을 처리하는 일반적인 시나리오입니다. 허용 목록은 광범위한 규칙으로 간주됩니다. 거짓 부정의 가능성을 줄이려면 경로 또는 헤더 일치와 같이 더 세분화된 다른 옵션과 페어링하는 것이 좋습니다.

IP 기반 제어

단일 IP 주소 블록

봇의 영향을 완화하는 데 일반적으로 사용되는 도구는 단일 요청자의 요청을 제한하는 것입니다. 가장 간단한 예는 요청이 악성이거나 볼륨이 많은 경우 트래픽의 소스 IP 주소를 차단하는 것입니다. IP 세트 일치 규칙을 사용하여 AWS WAF IP 기반 블록을 구현합니다. 이러한 규칙은 IP 주소와 일치하며 `Block`, `Challenge`또는 작업을 적용합니다CAPTCHA. 콘텐츠 전송 네트워크(CDN), 웹 애플리케이션 방화벽 또는 애플리케이션 및 서비스 로그를 확인하여 IP 주소에서 너무 많은 요청이 들어오는 시기를 확인할 수 있습니다. 그러나 대부분의 경우이 제어는 자동화 없이는 실용적이지 않습니다.

에서 IP 주소 블록 목록 자동화 AWS WAF 는 일반적으로 속도 기반 규칙을 사용하여 수행됩니다. 자세한 내용은 이 안내서의 속도 기반 규칙 섹션을 참조하세요. 솔루션을 위한 보안 자동화 AWS WAF를 구현할 수도 있습니다. 이 솔루션은 차단할 IP 주소 목록을 자동으로 업데이트하고 AWS WAF 규칙은 해당 IP 주소와 일치하는 요청을 거부합니다.

봇 공격을 인식하는 한 가지 방법은 동일한 IP 주소의 여러 요청이 소수의 웹 페이지에 초점을 맞추는 경우입니다. 이는 봇이 가격을 스크레이핑하거나 높은 비율로 실패하는 로그인을 반복적으로 시도하고 있음을 나타냅니다. 이 패턴을 즉시 인식하는 자동화를 생성할 수 있습니다. 자동화는 IP 주소를 차단하여 공격을 신속하게 식별하고 완화하여 공격의 효율성을 줄입니다. 공격자가 공격을 시작할 IP 주소 모음이 많거나 공격 동작을 인식하고 일반 트래픽과 분리하기 어려운 경우 특정 IP 주소를 차단하는 것은 덜 효과적입니다.

IP 주소 평판

IP 평판 서비스는 IP 주소의 신뢰성을 평가하는 데 도움이 되는 인텔리전스를 제공합니다. 이 인텔리전스는 일반적으로 해당 IP 주소의 과거 활동에서 IP 관련 정보를 집계하여 파생됩니다. 이전 활동은 IP 주소가 악의적인 요청을 생성할 가능성을 나타내는 데 도움이 됩니다. 데이터는 IP 주소 동작을 추적하는 관리형 목록에 추가됩니다.

익명 IP 주소는 IP 주소 평판의 특수한 사례입니다. 소스 IP 주소는 클라우드 기반 가상 머신과 같이 쉽게 획득할 수 있는 IP 주소의 알려진 소스 또는 알려진 VPN 공급자 또는 Tor 노드와 같은 프록시에서 비롯됩니다. AWS WAF Amazon IP 평판 목록 및 익명 IP 목록 관리형 규칙 그룹은 Amazon 내부 위협 인텔리전스를 사용하여 이러한 IP 주소를 식별하는 데 도움이 됩니다.

이러한 관리형 목록에서 제공하는 인텔리전스는 이러한 소스에서 식별된 활동에 대해 조치를 취하는 데 도움이 될 수 있습니다. 이 인텔리전스를 기반으로 트래픽을 직접 차단하는 규칙 또는 요청 수를 제한하는 규칙(예: 속도 기반 규칙)을 생성할 수 있습니다. 또한이 인텔리전스를 사용하여 COUNT 모드의 규칙을 사용하여 트래픽 소스를 평가할 수 있습니다. 그러면 일치 기준이 검사되고 사용자 지정 규칙을 생성하는 데 사용할 수 있는 레이블이 적용됩니다.

속도 기반 규칙

속도 기반 규칙은 특정 시나리오에 유용한 도구일 수 있습니다. 예를 들어, 속도 기반 규칙은 민감한 URIs(Uniform Resource Identifier)의 사용자와 비교하여 봇 트래픽이 대량에 도달하거나 트래픽 볼륨이 정상 작업에 영향을 미치기 시작할 때 유효합니다. 속도 제한은 요청을 관리 가능한 수준으로 유지하고 액세스를 제한 및 제어할 수 있습니다. AWS WAF 는 속도 기반 규칙 문을 사용하여 웹 액세스 제어 목록(웹 ACL)에서 속도 제한 규칙을 구현할 수 있습니다. https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html 속도 기반 규칙을 사용할 때 권장되는 접근 방식은 전체 사이트, URI별 규칙 및 IP 평판 속도 기반 규칙을 포함하는 포괄적 규칙을 포함하는 것입니다. IP 평판 속도 기반 규칙은 IP 주소 평판의 인텔리전스와 속도 제한 기능을 결합합니다.

전체 사이트의 경우 포괄적인 IP 평판 비율 기반 규칙은 정교한 봇이 적은 수의 IPs에서 사이트를 플러딩하지 못하도록 하는 상한을 생성합니다. 속도 제한은 로그인 또는 계정 생성 페이지와 같이 비용이나 영향이 높은 URIs를 보호하는 데 특히 권장됩니다.

속도 제한 규칙은 비용 효율적인 첫 번째 방어 계층을 제공할 수 있습니다. 고급 규칙을 사용하여 민감한 URIs. URI별 속도 기반 규칙은 데이터베이스 액세스와 같이 백엔드에 APIs에 미치는 영향을 제한할 수 있습니다. 이 가이드의 뒷부분에서 설명하는 특정 URIs를 보호하기 위한 고급 완화 조치에는 종종 추가 비용이 발생하며 이러한 URI별 속도 기반 규칙은 비용을 제어하는 데 도움이 될 수 있습니다. 일반적으로 권장되는 속도 기반 규칙에 대한 자세한 내용은 AWS 보안 블로그의 가장 중요한 세 가지 AWS WAF 속도 기반 규칙을 참조하세요. 경우에 따라 속도 기반 규칙으로 평가되는 요청 유형을 제한

하는 것이 유용합니다. 범위 축소 문을 사용하여 예를 들어 소스 IP 주소의 지리적 영역별로 비율 기반 규칙을 제한할 수 있습니다.

AWS WAF 는 집계 키를 사용하여 속도 기반 규칙에 대한 고급 기능을 제공합니다. 이 기능을 사용하면 소스 IP 주소 외에 다른 다양한 집계 키와 키 조합을 사용하도록 속도 기반 규칙을 구성할 수 있습니다. 예를 들어 단일 조합으로 전달된 IP 주소, HTTP 메서드 및 쿼리 인수를 기반으로 요청을 집계할 수 있습니다. 이를 통해 정교한 볼륨 측정 트래픽 완화를 위해 보다 세분화된 규칙을 구성할 수 있습니다.

내장 검사

내장 검사는 시스템 또는 프로세스 내에서 다양한 유형의 내부 또는 내재적 검증 또는 확인입니다. 봇 제어 AWS WAF 의 경우는 요청에 전송된 정보가 시스템 신호와 일치하는지 확인하여 내장 검사를 수행합니다. 예를 들어 역방향 DNS 조회 및 기타 시스템 확인을 수행합니다. SEO 관련 요청과 같은 일부 자동 요청이 필요합니다. 허용 목록은 양호하고 예상되는 봇을 허용하는 방법입니다. 그러나 악의적인 봇이 좋은 봇을 에뮬레이션하는 경우가 있으며, 이를 분리하는 것은 어려울 수 있습니다.는 관리형 AWS WAF Bot Control 규칙 그룹을 통해 이를 수행하는 방법을 AWS WAF 제공합니다. 이 그룹의 규칙은 자체 식별 봇이 누구인지 확인합니다.는 요청의 세부 정보를 해당 봇의 알려진 패턴과 비교하여 AWS WAF 확인하고 역방향 DNS 조회 및 기타 목표 확인도 수행합니다.

봇 관리를 위한 클라이언트 식별 제어

정적 속성을 통해 공격 관련 트래픽을 쉽게 인식할 수 없는 경우, 탐지를 통해 요청을 하는 클라이언트를 정확하게 식별할 수 있어야 합니다. 예를 들어 속도 제한 속성이 쿠키 또는 토큰과 같은 애플리케이션별로 다르면 속도 기반 규칙이 더 효과적이고 회피하기 어려운 경우가 많습니다. 세션에 연결된 쿠키를 사용하면 봇넷 운영자가 여러 봇에서 유사한 요청 흐름을 복제할 수 없습니다.

토큰 획득은 일반적으로 클라이언트 식별에 사용됩니다. 토큰 획득을 위해 JavaScript 코드는 정보를 수집하여 서버 측에서 평가되는 토큰을 생성합니다. 평가는 클라이언트에서 JavaScript가 실행 중인지 확인하는 것부터 지문을 위한 디바이스 정보를 수집하는 것까지 다양할 수 있습니다. 토큰을 획득하려면 JavaScript SDK를 사이트 또는 애플리케이션에 통합하거나 서비스 공급자가 동적으로 삽입을 수행해야 합니다.

JavaScript 지원을 요구하면 브라우저를 에뮬레이션하려는 봇에 대한 추가 장애물이 추가됩니다. 모바일 애플리케이션과 같이 SDK가 관련된 경우 토큰 획득은 SDK 구현을 확인하고 봇이 애플리케이션의 요청을 모방하지 못하도록 합니다.

토큰을 획득하려면 연결의 클라이언트 측에서 구현된 SDKs를 사용해야 합니다. 다음 AWS WAF 기능은 브라우저용 JavaScript 기반 SDK와 모바일 디바이스용 애플리케이션 기반 SDK를 제공합니다. Bot Control, Fraud Control 계정 탈취 방지(ATP) 및 Fraud Control 계정 생성 사기 방지(ACFP).

클라이언트 식별 기법에는 CAPTCHA, 브라우저 프로파일링, 디바이스 지문 및 TLS 지문이 포함됩니다.

CAPTCHA

컴퓨터와 인간을 구분하는 완전 자동화된 퍼블릭 Turing 테스트(CAPTCHA)는 로봇 방문자와 인간 방문자를 구분하고 웹 스크레이핑, 자격 증명 스터핑 및 스팸을 방지하는 데 사용됩니다. 구현은 다양하지만 사람이 해결할 수 있는 퍼즐이 포함되는 경우가 많습니다. CAPTCHAs 일반적인 봇에 대한 추가 방어 계층을 제공하며 봇 탐지의 오탐을 줄일 수 있습니다.

AWS WAF 를 사용하면 규칙이 규칙의 검사 기준과 일치하는 웹 요청에 대해 CAPTCHA 작업을 실행할 수 있습니다. 이 작업은 서비스에서 수집한 클라이언트 식별 정보를 평가한 결과입니다. AWS WAF 규칙은 로그인, 검색 및 양식 제출과 같이 봇이 자주 대상으로 하는 특정 리소스에 대해 CAPTCHA 문제를 해결해야 할 수 있습니다.는 중간 수단을 통해 또는 SDK를 사용하여 클라이언트 측에서 처리함으로써 CAPTCHA를 직접 제공할 AWS WAF 수 있습니다. 자세한 내용은 CAPTCHA 및 Challenge in AWS WAF을 참조하세요.

브라우저 프로파일링

브라우저 프로파일링은 대화형 브라우저를 사용하여 실제 인간을 분산된 봇 활동과 구별하기 위해 토큰 획득의 일부로 브라우저 특성을 수집하고 평가하는 방법입니다. 브라우저 작동 방식에 고유한 헤더, 헤더 순서 및 기타 요청 특성을 통해 브라우저 프로파일링을 수동적으로 수행할 수 있습니다.

토큰 획득을 사용하여 코드에서 브라우저 프로파일링을 수행할 수도 있습니다. 브라우저 프로파일링에 JavaScript를 사용하면 클라이언트가 JavaScript를 지원하는지 빠르게 확인할 수 있습니다. 이를 통해 이를 지원하지 않는 간단한 봇을 감지할 수 있습니다. 브라우저 프로파일링은 HTTP 헤더 및 JavaScript 지원 이상의 검사를 수행합니다. 브라우저 프로파일링은 봇이 웹 브라우저를 완전히 에뮬레이션하기 어렵게 만듭니다. 두 브라우저 프로파일링 옵션 모두 동일한 목표가 있습니다. 즉, 브라우저 프로파일에서 실제 브라우저의 동작 방식과 불일치를 나타내는 패턴을 찾는 것입니다.

AWS WAF 대상 봇에 대한 봇 제어는 토큰 평가의 일부로 브라우저가 자동화 또는 일관되지 않은 신호의 증거를 표시하는지 여부를 나타냅니다.는 규칙에 지정된 작업을 수행하기 위해 요청을 AWS WAF 지연시킵니다. 자세한 내용은 AWS 보안 블로그의 고급 봇 트래픽 감지 및 차단을 참조하세요.

디바이스 지문

디바이스 지문은 브라우저 프로파일링과 유사하지만 브라우저에만 국한되지 않습니다. 디바이스(모바일 디바이스 또는 웹 브라우저일 수 있음)에서 실행되는 코드는 디바이스의 세부 정보를 수집하여 백엔

드 서버에 보고합니다. 세부 정보에는 메모리, CPU 유형, 운영 체제(OS) 커널 유형, OS 버전 및 가상화와 같은 시스템 속성이 포함될 수 있습니다.

디바이스 지문을 사용하여 봇이 환경을 에뮬레이션하는지 또는 자동화가 사용 중이라는 직접적인 징후가 있는지 확인할 수 있습니다. 이 외에도 디바이스 지문을 사용하여 동일한 디바이스에서 반복되는 요청을 인식할 수도 있습니다.

디바이스가 요청의 일부 특성을 변경하려고 하더라도 동일한 디바이스에서 반복된 요청을 인식하면 백엔드 시스템이 속도 제한 규칙을 적용할 수 있습니다. 디바이스 지문을 기반으로 하는 속도 제한 규칙은 일반적으로 IP 주소를 기반으로 하는 속도 제한 규칙보다 더 효과적입니다. 이를 통해 VPNs 또는 프록시 간에 순환하지만 소수의 디바이스에서 소싱되는 봇 트래픽을 완화할 수 있습니다.

애플리케이션 통합 SDKs와 함께 사용하면 대상 AWS WAF 봇에 대한 봇 제어가 클라이언트 세션 요청 동작을 집계할 수 있습니다. 이렇게 하면 둘 다 동일한 IP 주소에서 시작되더라도 합법적인 클라이언트 세션을 감지하고 악성 클라이언트 세션과 분리할 수 있습니다. 대상 AWS WAF 봇의 봇 제어에 대한 자세한 내용은 AWS 보안 블로그의 고급 봇 트래픽 감지 및 차단을 참조하세요.

TLS 지문

서명 기반 규칙이라고도 하는 TLS 지문은 봇이 많은 IP 주소에서 시작되지만 유사한 특성을 보일 때 일반적으로 사용됩니다. HTTPS를 사용하는 경우 클라이언트와 서버 측은 메시지를 교환하여 서로를 확인하고 확인합니다. 암호화 알고리즘과 세션 키를 설정합니다. 이를 TLS 핸드셰이크라고 합니다. TLS 핸드셰이크를 구현하는 방법은 많은 IP 주소에 분산된 대규모 공격을 인식하는 데 유용한 서명입니다.

TLS 지문을 사용하면 웹 서버가 높은 정확도로 웹 클라이언트의 ID를 확인할 수 있습니다. 애플리케이션 데이터 교환이 발생하기 전에 첫 번째 패킷 연결에 파라미터만 필요합니다. 이 경우 웹 클라이언트는 요청을 시작하는 애플리케이션을 나타내며, 브라우저, CLI 도구, 스크립트(봇), 기본 애플리케이션 또는 기타 클라이언트일 수 있습니다.

SSL 및 TLS 지문 접근 방식 중 하나는 JA3 지문입니다. JA3는 SSL 또는 TLS 핸드셰이크의 클라이언트 Hello 메시지에 있는 필드를 기반으로 클라이언트 연결을 지문으로 만듭니다. 이를 통해 다양한 소스 IP 주소, 포트 및 X.509 인증서에서 특정 SSL 및 TLS 클라이언트를 프로파일링할 수 있습니다.

Amazon CloudFront는 요청에 JA3 헤더 추가를 지원합니다. `CloudFront-Viewer-JA3-Fingerprint` 헤더에는 수신되는 최종 사용자 요청의 TLS Client Hello 패킷의 32자 해시 지문이 포함되어 있습니다. 지문은 클라이언트가 통신하는 방법에 대한 정보를 캡슐화합니다. 이 정보는 동일한 패턴을 공유하는 클라이언트를 프로파일링하는 데 사용할 수 있습니다. 오리진 요청 정책에 `CloudFront-Viewer-JA3-Fingerprint` 헤더를 추가하고 정책을 CloudFront 배포에 연결할 수 있습니다. 그런 다음 오리진 애플리케이션 또는 Lambda@Edge 및 CloudFront 함수에서 헤더 값을 검사

할 수 있습니다. 헤더 값을 알려진 멀웨어 지문 목록과 비교하여 악성 클라이언트를 차단할 수 있습니다. 또한 헤더 값을 예상 지문 목록과 비교하여 알려진 클라이언트의 요청만 허용할 수 있습니다.

봇 관리를 위한 고급 분석 제어

일부 봇은 고급 기만 도구를 사용하여 탐지를 적극적으로 회피합니다. 이러한 봇은 머리카락과 같은 특정 활동을 수행하기 위해 사람의 행동을 모방합니다. 이러한 봇은 목적이 있으며 일반적으로 큰 금전적 보상과 연결됩니다.

이러한 고급 영구 봇은 다양한 기술을 사용하여 탐지를 회피하거나 정기적인 트래픽과 혼합합니다. 따라서 악성 트래픽을 정확하게 식별하고 완화하려면 다양한 탐지 기술을 혼합해야 합니다.

대상 사용 사례

사용 사례 데이터는 봇 감지 기회를 제공할 수 있습니다. 사기 탐지는 특별한 완화 조치가 필요한 특별한 사용 사례입니다. 예를 들어 계정 탈취를 방지하기 위해 손상된 계정 사용자 이름 및 암호 목록을 로그인 또는 계정 생성 요청과 비교할 수 있습니다. 이렇게 하면 웹 사이트 소유자가 손상된 자격 증명을 사용하는 로그인 시도를 감지할 수 있습니다. 손상된 자격 증명을 사용하면 봇이 계정을 맡으려고 하거나 자격 증명이 손상되었음을 알지 못하는 사용자일 수 있습니다. 이 사용 사례에서 웹 사이트 소유자는 추가 단계를 수행하여 사용자를 확인한 다음 암호를 변경하도록 도울 수 있습니다.는이 사용 사례에 대한 사기 제어 계정 탈취 방지(ATP) 관리형 규칙을 AWS WAF 제공합니다.

애플리케이션 수준 또는 집계된 봇 감지

일부 사용 사례에서는 콘텐츠 전송 네트워크(CDN)의 요청 AWS WAF과 애플리케이션 또는 서비스의 백엔드에 대한 데이터를 결합해야 합니다. 봇에 대해 높은 신뢰도의 결정을 내릴 수 있도록 타사 인텔리전스를 통합해야 하는 경우가 있습니다.

Amazon CloudFront 및의 기능은 백엔드 인프라에 신호를 AWS WAF 보내거나 이후에 헤더와 레이블을 통해 규칙을 집계할 수 있습니다. CloudFront는 앞서 언급한 대로 JA3 지문 헤더를 노출합니다. 다음은 헤더를 통해 이러한 데이터를 제공하는 CloudFront의 예입니다.는 규칙과 일치할 때 레이블을 전송할 AWS WAF 수 있습니다. 후속 규칙은 이러한 레이블을 사용하여 봇에 대한 더 나은 결정을 내릴 수 있습니다. 여러 규칙을 결합하면 매우 세분화된 제어를 구현할 수 있습니다. 일반적인 사용 사례는 레이블을 통해 관리형 규칙의 일부와 일치시킨 다음 다른 요청 데이터와 결합하는 것입니다. 자세한 내용은 AWS WAF 설명서의 레이블 일치 예제를 참조하세요.

기계 학습 분석

머신 린닝(ML)은 봇을 처리하는 강력한 기술입니다. ML은 변화하는 세부 정보에 적응할 수 있으며, 다른 도구와 결합하면 오탐을 최소화하면서 봇을 완화할 수 있는 가장 강력하고 완전한 방법을 제공합니다. 가장 일반적인 두 가지 ML 기법은 동작 분석과 이상 탐지입니다. 동작 분석을 통해 시스템(클라이언트, 서버 또는 둘 다)은 사용자가 애플리케이션 또는 웹 사이트와 상호 작용하는 방식을 모니터링합니다. 마우스 이동 패턴 또는 클릭 및 터치 상호 작용 빈도를 모니터링합니다. 그런 다음 ML 모델로 동작을 분석하여 봇을 인식합니다. 이상 탐지는 비슷합니다. 애플리케이션 또는 웹 사이트에 정의된 기준과 크게 다른 동작 또는 패턴을 감지하는 데 중점을 둡니다.

AWS WAF 봇의 대상 제어는 예측 ML 기술을 제공합니다. 이 기술은 탐지를 회피하도록 설계된 봇이 수행하는 분산된 프록시 기반 공격으로부터 보호하는 데 도움이 됩니다. 관리형 AWS WAF Bot Control 규칙 그룹은 웹 사이트 트래픽 통계에 대한 자동화된 ML 분석을 사용하여 분산되고 조정된 봇 활동을 나타내는 변칙적인 동작을 감지합니다.

봇 제어 전략의 배포 및 구현

봇 제어 배포 전략을 계획할 때 고려해야 할 여러 요소가 있습니다. 웹 애플리케이션의 고유한 특성 외에도 환경 크기, 개발 프로세스 및 조직 구조가 배포 전략에 영향을 미칩니다. 환경 및 애플리케이션 특성에 따라 중앙 집중식 또는 분산형 배포 전략을 사용할 수 있습니다.

- 중앙 집중식 배포 전략 - 중앙 집중식 접근 방식을 사용하면 봇 제어를 엄격하게 적용하려는 경우 더 높은 수준의 제어를 사용할 수 있습니다. 이 접근 방식은 애플리케이션 팀이 관리를 오프로드하려는 경우에 적합합니다. 중앙 집중식 접근 방식은 웹 애플리케이션이 유사한 특성을 공유할 때 가장 효과적입니다. 이 경우 애플리케이션은 일반적인 봇 제어 규칙 세트와 봇 완화 작업의 이점을 누릴 수 있습니다.
- 분산형 배포 전략 - 분산형 접근 방식은 애플리케이션 팀에 봇 제어 구성을 독립적으로 정의하고 구현할 수 있는 자율성을 제공합니다. 이 접근 방식은 소규모 환경이나 애플리케이션 팀이 봇 제어 정책에 대한 제어를 유지해야 하는 경우에 일반적입니다. 많은 웹 애플리케이션의 특성으로 인해 고유한 애플리케이션 특성에 맞게 조정된 독립적인 봇 제어 정책을 유지해야 하는 경우가 많으므로 분산된 접근 방식이 가능합니다.
- 결합된 전략 - 이러한 두 접근 방식의 조합은 웹 애플리케이션을 혼합하는 데 적합합니다. 예를 들어, 여기에는 모든 웹 ACLs에 적용되는 기본 규칙 세트가 수반될 수 있지만 보다 구체적인 봇 제어 정책의 관리는 애플리케이션 팀에 위임됩니다.

AWS Firewall Manager를 사용하여 봇 제어 정책을 정의하는 AWS WAF 웹 ACLs를 중앙 집중화하고 자동화할 수 있습니다. Firewall Manager를 사용할 때는 애플리케이션 팀에 위임해야 하는지 여부를 포함하여 봇 제어 정책을 중앙 집중화하는 것이 적절한지 고려합니다. Firewall Manager를 사용하면 태그 지정을 사용하여 애플리케이션 팀이 AWS WAF 정책을 옵트인할 수 있습니다. 이를 통해 지능형 위협 완화 기능을 AWS WAF 제공합니다. 애플리케이션 및 보안 작업에 대한 중앙 집중식 AWS WAF 로깅을 활성화할 수도 있습니다.

사용되는 배포 전략에 관계없이 또는와 같은 AWS CloudFormation 코드형 인프라(IaC) 기반 프레임워크를 통해 온보딩 프로세스를 정의하고 관리하는 것이 좋습니다AWS Cloud Development Kit (AWS CDK). 이렇게 하면 구성 객체를 저장하고 버전 관리하도록 소스 제어를 구성할 수 있습니다. 자세한 내용은 AWS CDK (GitHub) 및 CloudFormation(AWS 문서)에 대한 AWS WAF 구성 샘플을 참조하세요.

구현 전략

배포 전략을 선택한 후 구현을 시작할 수 있습니다. 배포 전략은 규칙이 여러 애플리케이션에 롤아웃되는 방법을 정의합니다. 구현 전략에서는 제어를 추가하고, 테스트하고, 지속적으로 모니터링하고, 효과를 평가하는 반복적인 프로세스에 중점을 둡니다.

트래픽 패턴 이해

트래픽 패턴을 실제로 이해하려면 애플리케이션의 비즈니스 기능과 사용 패턴, 주요 리소스, 사용자 페르소나와 같은 예상 속성을 숙지하는 것이 중요합니다. 프로덕션 트래픽과 애플리케이션에 대한 테스트 중에 생성된 트래픽을 통합하여 평가 기준을 설정합니다. 타임프레임에 여러 사용량 피크를 충분히 나타내는 트래픽 데이터가 포함되어 있는지 확인합니다.

선호하는 도구를 사용하여 대표 사용 기간 동안의 트래픽 로그 및 지표를 검토합니다. `headers` (예: `User-Agent` 및 `Referer`), `country`및와 같은 AWS WAF 로그 필드를 필터링하여 이상 요청에 대한 로그 데이터를 분석합니다`clientIp`. 균일한 리소스 식별자(URIs)와 액세스 빈도를 기록해 둡니다. 좋은 봇 식별과 같은 트래픽을 분류합니다. 예를 들어 검색 엔진 크롤러 및 모니터와 같은 유용한 봇에 대한 액세스를 허용합니다.

AWS WAF 콘솔의 봇 제어 대시보드에서 모든 활성 웹 ACL에 봇 활동 샘플을 사용할 수 있습니다. 이는 일반적인 봇 요청 볼륨에 대한 초기 관점을 제공하지만 봇 활동을 더 잘 이해하기 위해 추가 구성 및 분석을 수행합니다.

효과적인 구현을 위해서는 봇 트래픽과 그 효과, 그리고 어떤 봇 요청이 악의적 요청이 아닌 유익한지 잘 이해해야 합니다. 이렇게 하면 다음 단계에서 제어를 선택하고 봇 트래픽을 병렬로 평가하는 데 도움이 됩니다.

컨트롤 선택 및 추가

초기 트래픽 분석은 사용할 봇 제어와 각각에 대해 선택할 작업을 결정하는 데 도움이 됩니다. 잠재적인 향후 조치를 위해 활동을 기록하고 모니터링하도록 선택할 수도 있습니다. 초기 트래픽 분석은 트래픽을 관리하는 데 가장 적합한 제어를 선택하는 데 도움이 됩니다. 사용 가능한 컨트롤에 대한 자세한 내용은이 가이드봇 제어 기법의 섹션을 참조하세요.

이 단계에서 추가 SDK 구현을 포함하는 것이 좋습니다. 이를 통해 모든 필수 애플리케이션에서 SDK 구현을 테스트하고 완료할 수 있습니다. AWS WAF 봇 제어 및 사기 제어 규칙은 JavaScript SDK 또는 모바일 SDK를 구현할 때 완전한 토큰 평가 이점을 제공합니다. 자세한 내용은 AWS WAF 설명서의 Bot Control과 함께 애플리케이션 통합 SDKs를 사용해야 하는 이유를 참조하세요.

다음과 같이 다양한 애플리케이션 유형에 토큰 획득을 구현하는 것이 좋습니다.

- 단일 페이지 애플리케이션(SPA) - JavaScript SDK(리디렉션 없음)
- 모바일 브라우저 - JavaScript SDK 또는 규칙 작업(CAPTCHA 또는 챌린지)
- 웹 보기 - JavaScript SDK 또는 규칙 작업(CAPTCHA 또는 챌린지)
- 네이티브 애플리케이션 - Mobile SDK
- iFrames – JavaScript SDK

SDKs를 구현하는 방법에 대한 자세한 내용은 AWS WAF 설명서의 AWS WAF 클라이언트 애플리케이션 통합을 참조하세요.

프로덕션에 테스트 및 배포

제어는 처음에 테스트를 수행하여 예상 웹 애플리케이션 기능이 보존되었는지 확인할 수 있는 비프로덕션 환경에 배포해야 합니다. 프로덕션 배포 전에 항상 테스트 환경에서 철저한 검증을 수행합니다.

비프로덕션 환경에서 테스트 및 검증한 후 프로덕션 릴리스를 진행할 수 있습니다. 예상 사용자 트래픽이 가장 낮은 날짜와 시간을 선택합니다. 배포하기 전에 애플리케이션 및 보안 팀은 운영 준비 상태를 검토하고, 변경 사항을 롤백하는 방법을 논의하고, 대시보드를 검토하여 필요한 모든 지표와 경보가 구성되어 있는지 확인해야 합니다.

Amazon CloudFront 지속적 배포를 사용하면 봇 제어 평가를 위해 특별히 구성된 AWS WAF 웹 ACL이 있는 스테이징 배포로 소량의 트래픽을 보낼 수 있습니다.는 신규 또는 업데이트된 관리형 규칙의 버전 관리를 AWS WAF 제공하므로 프로덕션 트래픽 평가를 시작하기 전에 변경 사항을 테스트하고 승인할 수 있습니다.

제어 평가 및 튜닝

구현된 제어는 트래픽 활동 및 패턴에 대한 추가 인사이트와 가시성을 제공할 수 있습니다. 보안 제어를 추가하거나 조정하기 위해 애플리케이션 트래픽을 자주 모니터링하고 분석합니다. 일반적으로 잠재적 거짓 부정 및 거짓 긍정을 완화하기 위한 튜닝 단계가 있습니다. 거짓 부정은 컨트롤에 의해 포착되지 않아 규칙을 강화해야 하는 공격입니다. 거짓 긍정은 공격으로 잘못 식별되어 결과적으로 차단된 합법적인 요청을 나타냅니다.

분석 및 튜닝은 수동 또는 도구의 도움을 받아 수행할 수 있습니다. 보안 정보 및 이벤트 관리(SIEM) 시스템은 지표와 지능형 모니터링을 제공하는 데 도움이 되는 일반적인 도구입니다. 다양한 수준의 정교함으로 사용할 수 있는 많은 것이 있지만, 모두 트래픽 인사이트를 얻기 위한 좋은 출발점을 제공합니다.

웹 사이트 및 애플리케이션에 대한 중요한 핵심 성능 지표(KPIs 정의하면 사물이 예상대로 작동하지 않는 시점을 더 빠르게 식별하는 데 도움이 될 수 있습니다. 예를 들어, 봇이 생성할 수 있는 비즈니스 이상 징후의 지표로 신용 카드 환급, 계정당 매출 또는 전환율을 사용할 수 있습니다. 모니터링에 중요한 지표와 KPIs를 정의하고 이해하는 것은 모니터링 작업보다 훨씬 중요합니다.

봇 제어 솔루션에서 올바른 지표와 로그를 가져오는 방법을 이해하는 것은 모니터링할 지표를 식별하는 것만큼 중요합니다. 다음 섹션인 에서는 고려해야 할 모니터링 및 가시성 옵션을 봇 제어 전략 모니터링 지침자세히 설명합니다.

봇 제어 전략 모니터링 지침

봇 트래픽과 웹 애플리케이션 트래픽의 경우 모니터링과 가시성이 매우 중요합니다. 이는 보안 운영뿐만 아니라 활동의 우선 순위를 정하는 데 도움이 됩니다. 세부 로깅 또는 SIEM 시스템 사용이 불가능한 경우 선택한 솔루션 또는 공급업체에서 제공하는 기본 메트릭을 모니터링하는 것부터 시작하는 것이 좋습니다.

이러한 가시성은 위협 인텔리전스, 규칙 강화, 오탐지 문제 해결, 사고 대응에 유용합니다. 에서 사용할 수 있는 모니터링 옵션은 여러 가지가 있습니다. AWS WAF상위 수준 모니터링의 경우 에서 트래픽 개요 정보를 AWS WAF 제공합니다. AWS Management Console이는 웹 ACL에서 Bot Control 규칙 그룹이 활성화된 경우 모든 트래픽에 대해 사용할 수 있을 뿐만 아니라 봇 트래픽에 대한 세부 정보도 볼 수 있습니다.

AWS WAF 웹 ACL 트래픽의 세부 로깅을 위한 다양한 옵션을 제공합니다. 요청에 레이블을 추가하여 로그 분석을 용이하게 하고 봇 평가 규칙을 구성하는 데 사용할 수도 있습니다. Amazon CloudWatch Logs Insights를 통합하면 AWS WAF 로그를 쿼리하고 결과를 시각화할 수 있습니다.

세부 로깅을 켜면 사전 구성된 봇 AWS WAF 제어 대시보드 외에도 추가적인 가시성을 제공합니다. AWS WAF 로그를 사용하여 트래픽을 시각화하고 임시 조사를 수행하면 트래픽 패턴과 웹 애플리케이션의 완화 옵션을 심층적으로 이해할 수 있습니다.

Amazon CloudWatch Logs, Amazon Simple Storage 서비스 (Amazon S3) 또는 Amazon Data Firehose와 로그 데이터를 AWS WAF 통합할 수 있습니다. 자세한 내용은 AWS WAF 로깅 활성화 및 Amazon S3 또는 Amazon Data Firehose로 CloudWatch 로그 전송을 참조하십시오. Amazon OpenSearch Service 또는 AWS Marketplace솔루션을 비롯한 다양한 분석 대상으로 로그를 전송할 수도 있습니다. 자세한 내용은 Firehose 설명서의 대상 설정을 참조하십시오. 여러 로그 소스를 사용하는 경우 소스의 상관 관계를 파악할 수 있는 중앙 집중식 로깅 솔루션을 사용하는 것이 좋습니다.

다음으로 이 가이드에서는 Amazon을 사용하여 봇 트래픽 모니터링을 시작하고 가시성을 확보하는 방법에 대한 권장 사항을 제공합니다 CloudWatch.

주요 규칙 추적

가장 많이 사용되는 규칙을 추적하면 추세와 잠재적으로 변칙적인 활동을 파악할 수 있습니다. 특정 규칙의 비율이 증가하면 오탐이 발생하거나 표적 활동이 있을 수 있으므로 조사해야 합니다. 가장 일반적인 추적 규칙은 지역 차단 규칙 (이 규칙이 급증하면 자동으로 차단되지 않을 수 있는 특이한 국가의 트래픽이 표시될 수 있음) 및 입니다. IP 기반 제어 속도 기반 규칙 이러한 규칙에는 항상 변동이 따르지만

트래픽 패턴의 이상은 봇 활동을 의미할 수 있습니다. 임계값을 수동으로 설정하는 경우 이 점을 고려하십시오.

상위 레이블 및 네임스페이스 추적

CloudWatch 지표를 사용하여 상위 레이블을 추적하면 자주 호출되는 AWS WAF 규칙을 확인할 수 있습니다. 이를 통해 스크레이퍼 활동 증가, 의심스러운 소스로부터의 트래픽, 애플리케이션 로그인 페이지 또는 API의 남용 시도와 같은 이상 현상을 탐지할 수 있습니다.

관심을 가질만한 라벨의 예는 다음과 같습니다.

- `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`
- `awswaf:managed:aws:bot-control:bot:category:http_library`
- `awswaf:managed:aws:bot-control:bot:name:curl`
- `awswaf:managed:aws:atp:signal:credential_compromised`
- `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
- `awswaf:managed:token:rejected`

관심을 가질만한 레이블 네임스페이스의 예는 다음과 같습니다.

- `awswaf:managed:aws:bot-control:`
- `awswaf:managed:aws:atp:`
- `awswaf:managed:aws:anonymous-ip-list:`

수학 표현식 만들기

CloudWatchAmazon에서는 일부 또는 모든 규칙에 대해 수학 식을 생성할 수 있습니다. 수학 표현식에 알림을 설정하면 특정 지표의 수량이 아닌 비율의 이상 현상에 대한 알림을 받게 됩니다. 이는 알림 피로를 줄이는 데 중요한 도구입니다.

수학 식을 기반으로 사용자 지정 지표를 만드세요. 애플리케이션에 대한 전체 요청 수 중에서 규칙의 상대적 비율을 살펴보세요. 다음은 일반적인 수학 표현식입니다.

```
[ruleX count * 100]/[All allowed requests + All blocked requests]
```

이 수학 식은 백분율을 제공하므로 특정 규칙을 추적하고 시간 경과에 따른 추세를 시각화할 수 있습니다.

이상 탐지 사용

모든 CloudWatch 지표에서 CloudWatch예외 항목 탐지를 사용하면 실제 임계값을 수동으로 설정하지 않고도 비정상적으로 낮거나 높은 추세에 대한 알림을 제공할 수 있습니다. 이러한 알고리즘은 사용자 개입을 최소화하면서 시스템 및 애플리케이션의 메트릭을 지속적으로 분석하고, 정상 기준을 결정하고, 이상 현상을 찾아냅니다. CloudWatch 이상 탐지 기능에 통계 및 ML 알고리즘을 적용합니다.

아마존 CloudWatch 지표 사용

AWS WAF 트래픽을 처리하고 웹 ACL에 정의된 규칙과 일치하는 요청에 레이블을 추가합니다. 각 레이블은 지표를 생성합니다. CloudWatch 동시에 각 웹 ACL 규칙은 가능한 각 작업에 대한 지표도 생성합니다. 이러한 레이블 및 조치 지표를 사용하여 봇 트래픽을 고도로 이해하십시오. 이는 추세를 시각화하는 비용 효율적인 접근 방식입니다. 자세한 내용은 설명서에서 사용 가능한 지표 보기 및 그래프 지표를 참조하십시오. CloudWatch

CloudWatch 데이터를 로그 수집기 또는 집계자에게 보낼 수 있는 옵션을 제공합니다 (해당 AWS 서비스 솔루션이든 타사 솔루션이든). 에서 데이터를 수집하면 여러 소스의 데이터를 상호 CloudWatch 연관시킬 수 있는 보다 통합된 보안 관찰 경험을 제공할 수 있습니다. 이를 통해 알림 및 보안 자동화를 조사, 확인 또는 설정할 수 있습니다.

대시보드 구축

추적해야 할 중요한 지표를 식별한 후 가장 관련성이 높은 지표가 포함된 대시보드를 만드세요. 단일 창 아래에 side-by-side 표시하면 가시성과 제어력을 높일 수 있습니다.

비정상적인 지표 값에 대한 경고 및 자동화 규칙을 구성하는 것이 항상 좋습니다. 사람이 대시보드를 보고 이상 징후를 식별할 것이라고 기대하지 마십시오. 하지만 대시보드는 알림을 받은 후 조사 목적으로 유용할 수 있습니다.

봇 제어 전략의 비용 최적화

웹 트래픽의 특성은 동적입니다. 즉, 위협을 완화하는 데 사용되는 기술과 서비스는 다양하고 시간이 지남에 따라 조정될 수 있습니다. 이는 봇 제어 전략과 여기에 포함된 제어를 고려할 때 중요합니다. 시간 경과에 따른 최적화는 염두에 두어야 할 주요 원칙이며 AWS Well-Architected Framework의 비용 최적화 원칙에서 비롯됩니다.

AWS WAF 웹 ACLs 특히 새로운 기능이 출시되거나 새로운 위협을 완화하려는 경우 동적일 수 있습니다. 비용을 주시하려면 AWS WAF 서비스의 비용 차원과 각 차원이 최종 지출에 미치는 영향을 이해해야 합니다. 주요 주행 비용은 서비스에서 평가한 요청 수입니다. Bot Control 및 계정 탈취 방지(ATP) 관리형 규칙 그룹을 사용하거나 CAPTCHA 또는 챌린지와 같은 고급 작업을 사용하는 경우 추가 요금이 부과됩니다.

특수 봇 제어는 프리미엄 비용으로 제공되므로 기본 비용 최적화 목표는 이러한 고급 제어에서 검사하는 요청 수를 줄이는 것입니다. 적용 가능한 기법으로는 고부가가치 콘텐츠 분리, 저비용 측정 우선 적용, 평가 영역 범위 축소, 봇 보호와 다른 유형의 제어 결합 등이 있습니다. 비용 모니터링 기법은 조직 전체에 추가 가시성을 제공합니다.

동적 콘텐츠와 정적 콘텐츠 분리

한 가지 비용 절감 기법은 동적 애플리케이션에서 정적 콘텐츠를 격리하는 것입니다. 일반적인 웹 애플리케이션에 대한 대부분의 요청은 정적 객체에 대한 요청입니다. 애플리케이션 서버의 부하를 줄이는 일반적인 방법은 정적 콘텐츠를와 같은 자체 URL로 이동하는 것입니다`static.example.com`. 이는 정적 콘텐츠에 최적화된 캐싱 구성으로 고유한 콘텐츠 전송 배포를 생성하여 달성되는 경우가 많습니다. 또한이 기법은 정적 콘텐츠가 사이트 또는 애플리케이션에서 일반적으로 대상으로 지정되지 않는 경우 봇 제어 비용을 낮추는 데 도움이 될 수 있습니다. 동적 애플리케이션에서 정적 콘텐츠를 분리하면 고급 봇 제어를 보다 정밀하게 적용할 수 있습니다.

먼저 저렴한 규칙 적용

또 다른 기법은 고급 제어를 사용하기 전에 원치 않는 트래픽을 필터링하는 저비용 기준 규칙을 적용하는 것입니다. 실제로 이는 일반적으로 봇 제어 완화를 마지막 방어 계층으로 배치하고 이전 제어를 사용하여 원치 않는 트래픽을 필터링하는 것을 의미합니다.이 피라미드 접근 방식은 이전에이 가이드의 봇 제어 기법에서 설명했습니다. 주요 목표는 이러한 저비용 옵션을 사용하여 원치 않는 트래픽을 중지하는 것입니다. 그러면 고급 고비용 완화 기법으로 처리되는 요청 수가 줄어듭니다.

평가 영역 범위 축소

AWS WAF scope-down 문은 고급 규칙에서 검사하는 요청 수를 줄이는 강력한 기술을 제공합니다. 정적 콘텐츠를 자체 URL로 분리할 수 없는 경우, scope-down 문은 고급 완화 기술이 필요하지 않은 요청을 필터링하는 또 다른 방법입니다. 이는 특정 애플리케이션 경로, HTTP 메서드(예: POST) 또는 유사한 조합을 정의하여 수행할 수 있습니다.

봇 보호를 다른 컨트롤과 결합

원치 않는 봇 트래픽 외에도 여러 위협으로부터 애플리케이션을 보호할 때는 추가 비용 제어 고려 사항을 검토해야 합니다. 예를 들어 분산 서비스 거부(DDoS) 공격 및 계정 탈취로부터 보호하려면 비용에 영향을 미칠 수 있는 추가 구성이 필요합니다. Shield Advanced는 DDoS 공격으로부터 애플리케이션을 보호하는 데 도움이 되는 것이 좋습니다. 특히 애플리케이션 계층 완화는 요청 플러드를 자동으로 해결할 수 있으므로 규칙을 평가 순서에 앞서 배치할 때 Bot Control 규칙 그룹에서 처리할 AWS WAF 수 있는 요청 수를 줄일 수 있습니다. Shield Advanced에는 추가 이점이 있습니다. 표준 관리형 및 사용자 지정 AWS WAF 규칙은 Shield Advanced로 보호되는 리소스에 대해 추가 비용 없이 제공됩니다. Bot Control을 포함한 지능형 위협 완화 규칙 그룹에는 Shield Advanced로 보호되는 리소스에 대해서도 추가 비용이 발생합니다.

계정 탈취 방지가 필요한 애플리케이션은 AWS WAF 사기 제어 계정 탈취 방지(ATP) 규칙 그룹을 사용할 수 있습니다. ATP 규칙 그룹의 요청당 검사 비용은 Bot Control 규칙 그룹의 검사 비용보다 높습니다. 이렇게 비용이 높을수록 ATP 규칙 그룹을 최대한 정확하게 적용하는 것이 중요합니다. ATP와 함께 Bot Control 규칙 그룹을 사용하면이 목표를 달성하는 데 도움이 될 수 있습니다. 봇 요청을 필터링하고 ATP에서 검사하는 요청 수를 줄이려면 Bot Control 규칙 그룹을 웹 ACL의 ATP 앞에 배치해야 합니다.

지속적인 최적화를 위해 가장 중요한 활동은 Bot Control 규칙 그룹과 연결된 CloudWatch 지표를 모니터링하는 것입니다. 시간 경과에 따른 목표는 Bot Control 규칙 그룹이 평가한 요청 수를 원치 않는 봇 활동으로부터 보호하는 데 필요한 리소스를 대상으로 하는 요청 수로 줄이는 것입니다. CloudWatch 대시보드 구축은 AWS WAF 비용 및 사용량을 포함하여 애플리케이션에 대한 가장 중요한 지표의 가시성을 제공합니다.

비용 모니터링

AWS Cost Explorer는 비용 및 사용량을 보고 분석할 수 있게 해주는 도구입니다. Cost Explorer는 발생한 AWS 비용을 포함한 AWS WAF 비용 분석을 용이하게 합니다. 이 도구는 최근 12 개월 동안의 비용 정보를 제공하고 향후 12 개월 동안의 향후 지출을 예측합니다.

AWS 비용 이상 탐지는 비용 모니터링에 유용할 수 있는 또 다른 AWS WAF 비용 관리 제어 도구입니다. 고급 ML 기술을 사용하여 비정상적인 지출과 근본 원인을 식별합니다. 이렇게 하면 예상치 못한 비용 증가 시 신속하게 조치를 취하거나 알림을 받을 수 있습니다. 특정 비용 임계값에 도달하면 알림을 수신하기 위해 AWS Budgets는 해당 추적 및 모니터링 기능을 제공할 수 있습니다.

리소스

AWS 설명서

- AWS WAF 개발자 가이드
- AWS DDoS 복원력 모범 사례 (AWS 백서)
- 구현 AWS WAF지침 (백서)AWS

기타 리소스 AWS

- Amazon Logs의 AWS WAF CloudWatch 로그 분석 (AWS 블로그 게시물)
- 최소한의 AWS WAF 노력으로 대시보드를 배포하세요 (AWS 블로그 게시물)
- 보안 자동화 AWS WAF (AWS 솔루션 라이브러리)
- 가장 중요한 세 가지 AWS WAF 요금 기반 규칙 (AWS 블로그 게시물)
- Amazon CloudWatch 대시보드를 사용하여 AWS WAF 로그를 시각화하세요 (AWS 블로그 게시물)

기여자

작성

- 다이아나 알바라도, 선임 솔루션 아키텍트, AWS
- 캐머런 워렐, 엔터프라이즈 아키텍트, AWS
- 기어리 쉐러, 솔루션 아키텍트, AWS
- 초오리 타맘, 수석 솔루션 아키텍트, AWS

리뷰

- 제스 아이젠, 선임 소프트웨어 개발 엔지니어, AWS
- 카우스텁 파탁, 수석 제품 관리자, AWS
- 비크라마디티야 바트나가르, 선임 보안 컨설턴트, AWS

기술 문서 작성

- 릴리 AbouHarb, 선임 테크니컬 라이터, AWS

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2024년 2월 21일

AWS 권장 가이드 용어집

다음은 AWS 권장 가이드에서 제공하는 전략, 가이드 및 패턴에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하십시오.

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. 예: 온프레미스 Oracle 데이터베이스를 Amazon Aurora PostgreSQL 호환 에디션으로 마이그레이션합니다.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 AWS 클라우드의 Amazon Relational Database Service(Amazon RDS) for Oracle로 마이그레이션합니다.
- 재구매(드롭 앤드 숍) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com으로 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 AWS 클라우드클라우드의 EC2 인스턴스에 있는 Oracle로 마이그레이션합니다.
- 재배치(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 온프레미스 플랫폼에서 동일한 플랫폼의 클라우드 서비스로 서버를 마이그레이션합니다. 예: Microsoft Hyper-V 애플리케이션을 로 마이그레이션합니다 AWS.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중으로 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 참조하세요.

추상화된 서비스

관리형 서비스를 참조하세요.

ACID

원자성, 일관성, 격리성, 내구성을 참조하세요.

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 작동하고 그룹에 대한 단일 반환 값을 계산하는 SQL 함수입니다. 집계 함수의 예로 `SUM` 및 `MAX`가 있습니다.

AI

인공 지능을 참조하세요.

AIOps

인공 지능 운영을 참조하세요.

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

맬웨어로부터 시스템을 보호하기 위해 승인된 애플리케이션만 사용하도록 허용하는 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 탐색 및 분석 프로세스의 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 참조하십시오.

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 가이드를 참조하십시오.

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 용 ABAC AWS를 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 영역의 장애로부터 격리 AWS 리전 되고 동일한 리전의 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 내의 고유한 위치입니다.

AWS 클라우드 채택 프레임워크(AWS CAF)

조직이 클라우드로 성공적으로 전환 AWS 하기 위한 효율적이고 효과적인 계획을 개발하는 데 도움이 되는의 지침 및 모범 사례 프레임워크입니다. AWS CAF는 지침을 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영이라는 6가지 중점 영역으로 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 성공적인 클라우드 채택을 위해 조직을 준비하는 데 도움이 되는 인력 개발, 교육 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 AWS CAF 웹사이트와 AWS CAF 백서를 참조하세요.

AWS 워크로드 검증 프레임워크(AWS WQF)

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

B

악성 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

BCP

비즈니스 연속성 계획을 참조하세요.

동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그온 시도, 의심스러운 API 직접 호출 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 Data in a behavior graph를 참조하십시오.

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안도 참조하세요.

바이너리 분류

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

블룸 필터

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

블루/그린(Blue/Green) 배포

동일하지만 별개의 두 환경을 생성하는 배포 전략입니다. 하나의 환경(파란색)에서 현재 애플리케이션 버전을 실행하고 새 애플리케이션 버전은 다른 환경(녹색)에서 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 신속하게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 태스크를 실행하고 인적 활동이나 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같이 유용하거나 이로운 봇도 있습니다. 악성 봇이라고 하는 다른 일부 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

봇넷

맬웨어에 감염되고 봇 허더 또는 봇 운영자와 같은 단일 당사자가 제어하는 봇 네트워크입니다. 봇넷은 봇의 규모와 봇의 영향 범위를 확대하는 가장 잘 알려진 메커니즘입니다.

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 About branches(GitHub 설명서)를 참조하십시오.

긴급 액세스 권한

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는에 액세스할 수 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 AWS Well-Architected 지침의 Implement break-glass procedures 지표를 참조하세요.

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 AWS에서 컨테이너화된 마이크로서비스 실행의 비즈니스 역량 중심의 구성화 섹션을 참조하십시오.

비즈니스 연속성 계획(BCP)

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

C

CAF

AWS Cloud Adoption Framework를 참조하세요.

카나리 배포

최종 사용자에게 제공하는 느린 증분 릴리스 버전입니다. 확신이 들면 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

클라우드 혁신 센터를 참조하세요.

CDC

데이터 캡처 변경을 참조하세요.

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 중단 이벤트를 도입합니다. AWS Fault Injection Service (AWS FIS)를 사용하여 AWS 워크로드에 스트레스를 주고 응답을 평가하는 실험을 수행할 수 있습니다.

CI/CD

지속적 통합 및 지속적 전송을 참조하세요.

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

대상이 데이터를 AWS 서비스 수신하기 전에 로컬에서 데이터를 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 게시물을 참조하세요.

클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 엣지 컴퓨팅 기술에 연결되어 있습니다.

클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 클라우드 운영 모델 구축을 참조하십시오.

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 블로그 게시물 The Journey Toward Cloud-First and the Stages of Adoption on the AWS 클라우드 Enterprise Strategy 블로그에서 정의했습니다. AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 마이그레이션 준비 가이드를 참조하세요.

CMDB

구성 관리 데이터베이스를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리로 GitHub 또는 Bitbucket Cloud가 포함됩니다. 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(CV)

기계 학습을 사용하여 디지털 이미지 및 비디오와 같은 시각적 형식에서 정보를 분석하고 추출하는 AI 필드입니다. 예를 들어 Amazon SageMaker AI는 CV에 대한 이미지 처리 알고리즘을 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상되는 상태에서 변경됩니다. 이로 인해 워크로드가 규정을 준수하지 않을 수 있으며, 이는 일반적으로 점진적이고 의도되지 않은 작업입니다.

구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션의 포트폴리오 탐색 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 적합성 팩을 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 적합성 팩을 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 이점을 참조하십시오. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 지속적 전달(Continuous Delivery)과 지속적인 개발을 참조하십시오.

CV

컴퓨터 비전을 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 Framework의 보안 원칙 구성 요소입니다. 자세한 내용은 데이터 분류를 참조하십시오.

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 메시

중앙 집중식 관리 및 거버넌스를 통해 분산되고 탈중앙화된 데이터 소유권을 제공하는 아키텍처 프레임워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터를 최소화하면 개인 정보 보호 위험, 비용 및 분석 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 자격 증명만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경의 예방 가드레일 세트입니다. 자세한 내용은 데이터 경계 구축을 참조하세요 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 시스템입니다. 데이터 웨어하우스에는 보통 많은 양의 기록 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

데이터 정의 언어를 참조하세요.

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.

심층 방어

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. 이 전략을 채택하면 AWS Organizations 구조의 여러 계층에 여러 제어를 AWS추가하여 리소스를 보호할 수 있습니다. 예를 들어, 심층 방어 접근 방식은 다단계 인증, 네트워크 세분화 및 암호화를 결합할 수 있습니다.

위임된 관리자

에서 AWS Organizations호환되는 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 서비스를 참조하십시오.

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 참조하세요.

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 AWS에서 보안 제어 구현의 탐지 제어를 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.

차원 테이블

스타 스키마에서 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블을 말합니다. 차원 테이블 속성은 일반적으로 텍스트 필드나 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 보통 쿼리 제약, 필터링 및 결과 세트 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 가동 중지 시간 및 데이터 손실을 최소화하기 위해 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 Disaster Recovery of Workloads on AWS: Recovery in the Cloud를 참조하세요.

DML

데이터베이스 조작 언어를 참조하세요.

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 도메인 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 방법을 참조하십시오.

DR

재해 복구를 참조하세요.

드리프트 감지

기준이 되는 구성과의 편차 추적을 말합니다. 예를 들어 AWS CloudFormation 를 사용하여 시스템 리소스의 드리프트를 감지하거나를 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 랜딩 존의 변경 사항을 감지할 수 있습니다.

DVSM

개발 가치 흐름 매핑을 참조하세요.

E

EDA

탐색 데이터 분석을 참조하세요.

EDI

전자 데이터 교환을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 엣지 컴퓨팅은 클라우드 컴퓨팅에 비해 보다 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

전자 데이터 교환(EDI)

조직 간 비즈니스 문서의 자동화된 교환을 나타냅니다. 자세한 내용은 전자 데이터 교환(EDI)이란 무엇인가요?를 참조하세요.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 사이퍼텍스트로 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 참조하세요.

엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 를 사용하여 엔드포인트 서비스를 생성하고 다른 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 AWS PrivateLink 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 생성을 참조하십시오.

엔터프라이즈 리소스 계획(ERP)

엔터프라이즈의 주요 비즈니스 프로세스(예: 회계, MES, 프로젝트 관리)를 자동화하고 관리하는 시스템입니다.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service (AWS KMS) 설명서의 봉투 암호화를 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 대응이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 프로그램 구현 가이드를 참조하십시오.

ERP

엔터프라이즈 리소스 계획을 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 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블은 측정값이 있는 열 및 차원 테이블에 대한 외래 키가 있는 열과 같이 두 가지 열 유형을 포함합니다.

빠른 실패

개발 수명 주기를 줄이기 위해 빈번한 증분 테스트를 사용하는 철학입니다. 애자일 접근 방식의 핵심입니다.

장애 격리 경계

에서 장애의 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역, AWS 리전 컨트롤 플레인 또는 데이터 플레인과 같은 AWS 클라우드경계입니다. 자세한 내용은 AWS 장애 격리 경계를 참조하세요.

기능 브랜치

브랜치를 참조하세요.

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 그레디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

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 활용

할 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.

퓨샷 프롬프팅

유사한 태스크를 수행하도록 요청하기 전에 LLM에 태스크와 원하는 출력을 보여주는 몇 가지 예제를 제공합니다. 이 기법은 모델이 프롬프트에 포함된 예제(샷)에서 학습하는 컨텍스트 내 학습을 적용합니다. 퓨샷 프롬프팅은 특정 형식 지정, 추론 또는 분야별 지식이 필요한 태스크에 효과적일 수 있습니다. 제로샷 프롬프팅도 참조하세요.

FGAC

세분화된 액세스 제어를 참조하세요.

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계적 접근 방식을 사용하는 대신 변경 데이터 캡처를 통해 지속적 데이터 복제를 사용하여 최단 시간에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

파운데이션 모델을 참조하세요.

파운데이션 모델(FM)

일반화되고 레이블이 지정되지 않은 데이터의 대규모 데이터세트에서 훈련된 대규모 딥 러닝 신경망입니다. FM은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 태스크를 수행할 수 있습니다. 자세한 내용은 파운데이션 모델이란?을 참조하세요.

G

생성형 AI

대량의 데이터에서 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트, 오디오와 같은 새 콘텐츠와 아티팩트를 생성할 수 있는 AI 모델의 하위 세트입니다. 자세한 내용은 생성형 AI란 무엇인가요?를 참조하세요.

지리적 차단

지리적 제한을 참조하세요.

지리적 제한(지리적 차단)

Amazon CloudFront에서 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 옵션입니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 CloudFront 설명서의 콘텐츠의 지리적 배포 제한을 참조하십시오.

Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 트렁크 기반 워크플로는 선호되는 현대적 접근 방식입니다.

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 해당 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조 분야에서는 골든 이미지를 사용하여 여러 디바이스에서 소프트웨어를 프로비저닝할 수 있으며 이를 통해 딥이스 제조 작업의 속도, 확장성 및 생산성을 개선할 수 있습니다.

브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 브라운필드라고도 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, 이는 AWS Config,, Amazon GuardDuty AWS Security Hub CSPM, , AWS Trusted Advisor Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

H

HA

고가용성을 참조하세요.

이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스

키마를 변환하는 것은 복잡한 작업일 수 있습니다.AWS 는 스키마 변환에 도움이 되는 AWS SCT를 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.

홀드아웃 데이터

기계 학습 모델을 훈련하는 데 사용되는 데이터세트에서 보류되는 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교해 모델 성능을 평가할 수 있습니다.

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 리플랫포밍 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. 핫픽스는 긴급하기 때문에 일반적인 DevOps 릴리스 워크플로 외부에서 실행됩니다.

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

코드형 인프라를 참조하세요.

자격 증명 기반 정책

AWS 클라우드 환경 내에서 권한을 정의하는 하나 이상의 IAM 보안 주체에 연결된 정책입니다.

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 참조하세요.

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 또는 수정하는 대신 프로덕션 워크로드에 대한 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 변경 가능한 인프라보다 본질적으로 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 변경 불가능한 인프라를 사용하여 배포 모범 사례를 참조하세요.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부에서 네트워크 연결을 수락, 검사 및 라우팅하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

증분 마이그레이션

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

Industry 4.0

연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통해 제조 프로세스의 현대화를 나타내기 위해 2016년에 Klaus Schwab에서 도입한 용어입니다.

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 구축을 참조하십시오.

검사 VPC

AWS 다중 계정 아키텍처에서는 VPC(동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPCs입니다. AWS Security Reference Architecture에서는 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 참조하십시오.

해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

IoT

사물 인터넷을 참조하세요.

IT 정보 라이브러리(ITIL)

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

IT 서비스 관리(ITSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 운영을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

ITIL

IT 정보 라이브러리를 참조하세요.

ITSM

IT 서비스 관리를 참조하세요.

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 확장 가능하고 안전한 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 안전하고 확장 가능한 다중 계정 AWS 환경 설정을 참조하십시오.

대규모 언어 모델(LLM)

방대한 양의 데이터에서 사전 훈련된 딥 러닝 AI 모델입니다. LLM은 질문에 대한 답변, 문서 요약, 텍스트를 다른 언어로 번역, 문장 완성과 같은 여러 태스크를 수행할 수 있습니다. 자세한 내용은 대규모 언어 모델(LLM)이란 무엇인가요?를 참조하세요.

대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

레이블 기반 액세스 제어를 참조하세요.

최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 최소 권한 적용을 참조하십시오.

리프트 앤드 시프트

7R을 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안도 참조하세요.

LLM

대규모 언어 모델을 참조하세요.

하위 환경

환경을 참조하세요.

M

기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공 지능의 한 유형입니다. ML은 사물 인터넷(IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 기계 학습을 참조하십시오.

기본 브랜치

브랜치를 참조하세요.

맬웨어

컴퓨터 보안 또는 프라이버시를 위협하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 방해하거나 민감한 정보를 유출하거나 무단 액세스 권한을 확보할 수 있습니다. 맬웨어의 예로 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스 는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하고, 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. 관리형 서비스의 예로 Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB가 있습니다. 이를 추상화된 서비스라고도 합니다.

제조 실행 시스템(MES)

원자재를 생산 현장에서 완제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

Migration Acceleration Program을 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 조정을 위해 결과를 검사하는 전체 프로세스입니다. 메커니즘은 작동 시 자체적으로 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 메커니즘 구축을 참조하세요.

멤버 계정

조직의 일부인 관리 계정을 AWS 계정 제외한 모든 계정. AWS Organizations하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

MES

제조 실행 시스템을 참조하세요.

메시지 큐 원격 분석 전송(MQTT)

리소스 제약이 있는 IoT 디바이스에 대한 게시 및 구독 패턴을 기반으로 하는 경량 Machine-to-Machine(M2M) 통신 프로토콜입니다.

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 영역에 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 통합을 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 에서 마이크로서비스 구현을 참조하세요 AWS.

Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄하는 데 도움이 되는 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 전략의 세 번째 단계입니다.

마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 스프린트에서 일하는 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자, 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 가이드와 마이그레이션 팩토리에 대한 설명을 참조하십시오.

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. 예: AWS Application Migration Service를 사용하여 Amazon EC2로 마이그레이션을 리호스팅합니다.

Migration Portfolio Assessment(MPA)

AWS 클라우드로 마이그레이션하는 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 컨설턴트가 무료로 사용할 수 있습니다.

마이그레이션 준비 상태 평가(MRA)

AWS CAF를 사용하여 조직의 클라우드 준비 상태에 대한 인사이트를 얻고, 강점과 약점을 식별하고, 식별된 격차를 해소하기 위한 행동 계획을 수립하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 가이드를 참조하십시오. MRA는 AWS 마이그레이션 전략의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 AWS 클라우드로 마이그레이션하는 데 사용되는 접근 방식입니다. 자세한 내용은 이 용어집의 7R 항목과 조직을 동원하여 대규모 마이그레이션 가속화를 참조하세요.

ML

기계 학습을 참조하세요.

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 애플리케이션을 현대화하기 위한 전략을 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 평가를 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 분해를 참조하십시오.

MPA

Migration Portfolio Assessment를 참조하세요.

MQTT

메시지 큐 원격 분석 전송을 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 워크로드에 대한 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework에서는 변경 불가능한 인프라를 모범 사례로 사용할 것을 권장합니다.

O

OAC

오리진 액세스 제어를 참조하세요.

OAI

오리진 액세스 ID를 참조하세요.

OCM

조직 변경 관리를 참조하세요.

오프라인 마이그레이션

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

OI

운영 통합을 참조하세요.

OLA

운영 수준 계약을 참조하세요.

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.

OPC-UA

Open Process Communications - Unified Architecture(OPC-UA)를 참조하세요.

Open Process Communications - Unified Architecture(OPC-UA)

산업 자동화를 위한 Machine-to-Machine(M2M) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계에 관한 상호 운용성 표준을 제공합니다.

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 잠재적 장애의 범위를 이해, 평가 또는 예방하거나 줄이는 데 도움이 되는 질문 체크리스트 및 관련 모범 사례입니다. 자세한 내용은 AWS Well-Architected Framework의 운영 준비 상태 검토(ORR)를 참조하세요.

운영 기술(OT)

물리적 환경에서 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조 분야에서 OT 및 정보 기술(IT) 시스템의 통합은 Industry 4.0 트랜스포메이션의 주요 중점 사항입니다.

운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 운영 통합 가이드를 참조하십시오.

조직 트레일

조직 AWS 계정 내 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는에서 생성된 추적입니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정 에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서의 Creating a trail for an organization을 참조하십시오.

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 변경 속도 때문에이 프레임워크를 인력 가속화라고 합니다. 자세한 내용은 사용 가이드를 참조하십시오.

오리진 액세스 제어(OAC)

CloudFront에서 Amazon Simple Storage Service(S3) 콘텐츠를 보호하기 위해 액세스를 제한하는 고급 옵션입니다. OAC는 AWS KMS (SSE-KMS)를 사용한 모든 서버 측 암호화 AWS 리전와 S3 버킷에 대한 동적 PUT 및 DELETE 요청에서 모든 S3 버킷을 지원합니다.

오리진 액세스 ID(OAI)

CloudFront에서 Amazon S3 콘텐츠를 보호하기 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 CloudFront는 Amazon S3가 인증할 수 있는 보안 주체를 생성합니다. 인증된 보안 주체는 특

정 CloudFront 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. 더 세분화되고 향상된 액세스 제어를 제공하는 OAC도 참조하십시오.

ORR

운영 준비 상태 검토를 참조하세요.

OT

운영 기술을 참조하세요.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작된 네트워크 연결을 처리하는 VPC입니다. AWS Security Reference Architecture에서는 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 경계를 참조하십시오.

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 참조하세요.

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.

PLC

프로그래밍 가능 로직 컨트롤러를 참조하세요.

PLM

제품 수명 주기 관리를 참조하세요.

정책

권한 정의(ID 기반 정책 참조), 액세스 조건 지정(리소스 기반 정책 참조), AWS Organizations 내 조직의 모든 계정에 대한 최대 권한 정의(서비스 제어 정책 참조)와 같은 작업을 수행할 수 있는 객체입니다.

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 저장소를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 상태 평가를 참조하십시오.

조건자

보통 `WHERE` 절에 있는 `true` 또는 `false`를 반환하는 쿼리 조건입니다.

푸시다운 조건자

전송 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄고 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 controls를 참조하십시오.

보안 주체

작업을 수행하고 리소스에 액세스할 수 AWS 있는의 엔터티입니다. 이 엔터티는 일반적으로 , AWS 계정 IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 역할 용어 및 개념의 보안 주체를 참조하십시오.

개인 정보 보호 중심 설계

전체 개발 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 작업을 참조하십시오.

선제적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 제어는 리소스를 프로비저닝하기 전에 리소스를 스캔합니다. 리소스가 제어를 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 제어 참조 가이드를 참조하고 보안 제어 구현의 사전 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도를 거쳐 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리를 나타냅니다.

프로덕션 환경

환경을 참조하세요.

프로그래밍 가능 로직 컨트롤러(PLC)

제조 분야에서 기계를 모니터링하고 제조 프로세스를 자동화하는 매우 안정적이고 적응력이 뛰어난 컴퓨터입니다.

프롬프트 체이닝

한 LLM 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 태스크를 하위 태스크로 나누거나 예비 응답을 반복적으로 세부 조정하거나 확장하는 데 사용됩니다. 이를 통해 모델 응답의 정확성과 관련성을 개선하고 보다 세분화되고 개인화된 결과를 얻을 수 있습니다.

가명화

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

게시/구독(pub/sub)

여러 마이크로서비스에서 비동기 통신을 지원하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 MES에서 마이크로서비스는 다른 마이크로서비스가 구독할 수 있는 채널에 이벤트 메시지를 게시할 수 있습니다. 시스템은 게시 서비스를 변경하지 않고도 새 마이크로서비스를 추가할 수 있습니다.

Q

쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 명령어와 같은 일련의 단계입니다.

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

Responsible, Accountable, Consulted, Informed(RACI)를 참조하세요.

RAG

검색 증강 생성을 참조하세요.

랜섬웨어

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

RASCI 매트릭스

Responsible, Accountable, Consulted, Informed(RACI)를 참조하세요.

RCAC

행 및 열 액세스 제어를 참조하세요.

읽기 전용 복제본

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

리아키텍팅

7R을 참조하세요.

Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

Recovery Time Objective(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다.

리팩터링

7R을 참조하세요.

리전

지리적 영역의 AWS 리소스 모음입니다. 각 AWS 리전 는 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 계정에서 사용할 수 있는 AWS 리전 지정을 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

7R을 참조하세요.

릴리스

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

7R을 참조하세요.

리플랫포밍

7R을 참조하세요.

재구매

7R을 참조하세요.

복원력

중단에 저항하거나 중단을 복구할 수 있는 애플리케이션의 기능입니다. 고가용성 및 재해 복구는 AWS 클라우드에서 복원력을 계획할 때 일반적인 고려 사항입니다. 자세한 내용은 AWS 클라우드 복원력을 참조하세요.

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 조언자 (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 AWS에서 보안 제어 구현의 대응 제어를 참조하세요.

retain

7R을 참조하세요.

사용 중지

7R을 참조하세요.

검색 증강 세대(RAG)

응답을 생성하기 전에 LLM이 훈련 데이터 소스 외부에 있는 신뢰할 수 있는 데이터 소스를 참조하는 생성형 AI 기술입니다. 예를 들어 RAG 모델은 조직의 지식 기반 또는 사용자 지정 데이터에 대한 시맨틱 검색을 수행할 수 있습니다. 자세한 내용은 검색 증강 생성(RAG)이란 무엇인가요?를 참조하세요.

교체

공격자가 자격 증명에 액세스하는 것을 더욱 어렵게 만들기 위해 보안 암호를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

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

RPO

목표 복구 시점(RPO)을 참조하세요.

RTO

목표 복구 시간(RTO)을 참조하세요.

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(idP)에서 사용하는 개방형 표준입니다. 이 기능을 사용하면 연동 SSO(Single Sign-On)를 AWS Management Console 사용할 수 있으므로 사용자는 조직의 모든 사용자에 대해 IAM에서 사용자를 생성하지 않고도에 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 SAML 2.0 기반 페더레이션 정보를 참조하십시오.

SCADA

감독 제어 및 데이터 획득을 참조하세요.

SCP

서비스 제어 정책을 참조하세요.

보안 암호

에는 암호 또는 사용자 자격 증명과 같이 암호화된 형식으로 저장하는 AWS Secrets Manager기밀 또는 제한된 정보가 있습니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 AWS Secrets Manager 설명서의 Secrets Manager 보안 암호란 무엇인가요?를 참조하세요.

보안 중심 설계

전체 개발 프로세스에서 보안을 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어는 예방, 감지, 대응, 선제적과 같은 기본적인 네 가지 보안 제어 유형으로 구분됩니다.

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 응답 자동화

보안 이벤트에 자동으로 응답하거나 이를 해결하도록 설계된 사전 정의되고 프로그래밍된 작업입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 탐지 또는 대응 AWS 보안 제어 역할을 합니다. 자동화된 응답 작업의 예로 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치 적용 또는 자격 증명 교체 등이 있습니다.

서버 측 암호화

대상에서 데이터를 수신하는 AWS 서비스 에 의한 데이터 암호화.

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 정책을 참조하세요.

서비스 엔드포인트

에 대한 진입점의 URL입니다 AWS 서비스. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.

서비스 수준에 관한 계약(SLA)

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

서비스 수준 지표(SLI)

오류 발생률, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정값입니다.

서비스 수준 목표(SLO)

서비스 수준 지표로 측정되는 서비스의 상태를 나타내는 목표 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수를 AWS 위해와 공유하는 책임을 설명하는 모델입니다. AWS 는 클라우드의 보안을 담당하는 반면, 사용자는 클라우드의 보안을 담당합니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

SIEM

보안 정보 및 이벤트 관리 시스템을 참조하세요.

단일 장애점(SPOF)

애플리케이션을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소에서 발생하는 장애입니다.

SLA

서비스 수준 계약을 참조하세요.

SLI

서비스 수준 지표를 참조하세요.

SLO

서비스 수준 목표를 참조하세요.

분할 앤 시드 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 AWS 클라우드에서 애플리케이션을 현대화하기 위한 단계별 접근 방식을 참조하세요.

SPOF

단일 장애점을 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 더 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 데이터 웨어하우스에서 또는 비즈니스 인텔리전스 목적으로 사용하도록 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 Fowler가 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 방법을 참조하십시오.

서브넷

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

감독 제어 및 데이터 획득(SCADA)

제조 분야에서 하드웨어와 소프트웨어를 사용하여 물리적 자산과 프로덕션 작업을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

사용자 상호 작용을 시뮬레이션하여 잠재적 문제를 감지하거나 성능을 모니터링하는 방식으로 진행되는 시스템 테스트입니다. Amazon CloudWatch Synthetics를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

LLM에 컨텍스트, 명령 또는 지침을 제공하여 동작을 지시하는 기법입니다. 시스템 프롬프트는 컨텍스트를 설정하고 사용자와의 상호 작용을 위한 규칙을 설정하는 데 도움이 됩니다.

T

tags

AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색, 필터링할 수 있습니다. 자세한 내용은 AWS 리소스에 태그 지정을 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 참조하세요.

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.

Transit Gateway

VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 전송 게이트웨이란 무엇입니까?를 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 Organizations 및 해당 계정에서 조직에서 작업을 수행하도록 지정하는 서비스에 대한 권한 부여. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관리 작업을 수행합니다. 자세한 내용은 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요 AWS Organizations .

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 충분한 소규모 DevOps 팀. 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 참조하십시오.

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 참조하세요.

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 참조하십시오.

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.

창 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에서 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대적 위치를 기반으로 행 값에 액세스하는 등의 태스크를 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.

WORM

Write Once, Read Many(WORM)를 참조하세요.

WQF

AWS Workload Qualification Framework를 참조하세요.

Write Once Read Many(WORM)

데이터를 한 번 쓰고 데이터가 삭제되거나 수정되지 않도록 하는 스토리지 모델입니다. 권한 있는 사용자는 필요한 만큼 여러 번 데이터를 읽을 수 있지만 데이터를 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 변경 불가능한 항목으로 간주됩니다.

Z

제로데이 익스플로잇

[제로데이 취약성](#)을 악용하는 공격(일반적으로 맬웨어)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.

제로샷 프롬프팅

태스크를 수행하기 위해 [LLM](#)에 명령을 제공하지만 안내에 도움이 되는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 태스크를 처리해야 합니다. 제로샷 프롬프팅의 효과는 태스크의 복잡성과 프롬프트의 품질에 따라 달라집니다. [퓨샷 프롬프팅](#)도 참조하세요.

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.