AWS 스타트업 보안 베이스라인 (SSB)AWS

AWS 규범적 지침

AWS 규범적 지침: AWS 스타트업 보안 베이스라인 (SSB)AWS

Table of Contents

AWS Startup Security Baseline(AWS SSB)

Jay Michael, Amazon Web Services(AWS)

2023년 5월(문서 기록)

AWS Startup Security Baseline(SSB)은 AWS에서 기업이 민첩성을 저하시키지 않고 안전하게 구축할 수 있는 최소한의 기반을 만드는 제어 세트입니다. 이러한 제어는 보안 태세의 기반을 형성하며 보안 인증 보안, 로깅 및 가시성 지원, 연락처 정보 관리, 기본 데이터 경계 구현에 중점을 둡니다.

이 가이드의 제어 기능은 초기 시작을 염두에 두고 설계되었으므로 많은 노력을 기울이지 않고도 가장 일반적인 보안 위험을 완화할 수 있습니다. 많은 스타트업이 단일 AWS 계정로 AWS 클라우드에서 여정을 시작합니다. 조직이 성장함에 따라 다중 계정 아키텍처로 마이그레이션합니다. 이 가이드의 지침은 단일 계정 아키텍처용으로 설계되었지만 다중 계정 아키텍처로 전환할 때 쉽게 마이그레이션하거나 수정할 수 있는 보안 제어를 설정하는 데 도움이 됩니다.

AWS SSB의 제어는 계정과 워크로드라는 두 가지 범주로 구분됩니다. 계정 제어는 AWS 계정을 안전하게 유지하는 데 도움이 됩니다. 여기에는 사용자 액세스, 정책 및 권한 설정에 대한 권장 사항과 계정의 무단 또는 잠재적 악의적 활동을 모니터링하는 방법에 대한 권장 사항이 포함됩니다. 워크로드 제어는 애플리케이션, 백엔드 프로세스, 데이터 등 클라우드의 리소스와 코드를 보호하는 데 도움이 됩니다. 여기에는 암호화 및 액세스 범위 축소와 같은 권장 사항이 포함됩니다.

> **Note**
>
> 이 가이드에서 권장하는 일부 제어는 초기 설정 중에 구성된 기본값을 대체하지만 대부분은 새로운 설정과 정책을 구성합니다. 이 문서가 사용 가능한 모든 제어를 포괄하는 것으로 간주해서는 안 됩니다.

수강 대상

이 가이드는 최소한의 인력과 운영으로 개발 초기 단계에 있는 스타트업에 가장 적합합니다.

운영 및 성장의 후기 단계에 있는 스타트업이나 기타 비즈니스는 이러한 규제 항목을 현재 관행과 비교하여 검토함으로써 여전히 상당한 가치를 창출할 수 있습니다. 격차가 발견되면 이 가이드에 있는 개별 제어를 구현한 다음 장기 해결책으로서 적절성을 평가할 수 있습니다.

> **Note**
>
> 이 가이드의 권장 제어는 본질적으로 기본입니다. 스타트업이나 기타 규모나 정교화 단계에서 운영되는 기업은 해당되는 경우 제어 기능을 더 추가해야 합니다.

기본 프레임워크 및 보안 책임

AWS Well-Architected는 클라우드 아키텍트가 애플리케이션 및 워크로드를 위한 안전하고 성능 및 복원력이 뛰어나며 효율적인 인프라를 구축할 수 있도록 지원합니다. AWS Startup Security Baseline은 AWS Well-Architected Framework의 보안 원칙에 맞춰 조정됩니다. 보안 원칙은 보안 태세를 개선할 수 있는 방식으로 클라우드 기술을 활용하여 데이터, 시스템 및 자산을 보호하는 방법을 설명합니다. 현재 AWS 권장 사항에 따라 비즈니스 및 규제 요구 사항을 충족하는 데 도움이 됩니다.

AWS 계정에서 AWS Well-Architected Tool을 사용하여 Well-Architected 모범 사례를 준수하는지 평가할 수 있습니다.

보안과 규정 준수는 AWS와 고객의 공동 책임입니다. 공동 책임 모델은 AWS가 클라우드의 보안(즉, AWS 클라우드에서 제공되는 모든 서비스를 실행하는 인프라 보호)을 담당하고, 사용자가 클라우드 보안(선택한 AWS 클라우드 서비스에 따라 결정됨)을 담당한다는 말로 설명되는 경우가 많습니다. 공동 책임 모델에서 이 문서에 나와 있는 보안 제어를 구현하는 것은 고객 책임의 일부입니다.

계정 보안

이 섹션의 제어 및 권장 사항은 AWS 계정을 안전하게 유지하는 데 도움이 됩니다. 이 지침에서는 사람과 컴퓨터 액세스 모두에 AWS Identity and Access Management (IAM) 사용자, 사용자 그룹 및 역할 (보안 주체라고도 함) 을 사용하고, 루트 사용자의 사용을 제한하고, 다단계 인증을 요구하는 것을 강조합니다. 이 섹션에서는 계정 활동 및 상태와 관련하여 연락하는 AWS 데 필요한 연락처 정보가 있는지 확인합니다. 또한 Amazon GuardDuty 및 와 AWS Budgets같은 AWS Trusted Advisor모니터링 서비스를 설정하여 계정 활동에 대한 알림을 받고 활동이 승인되지 않았거나 예상치 못한 경우 신속하게 대응할 수 있습니다.

이 섹션은 다음 주제를 포함합니다:

ACCT.01 - 유효한 이메일 배포 목록으로 계정 수준의 연락처 설정

AWS 계정에 기본 연락처와 대체 연락처를 설정할 때는 개인의 이메일 주소 대신 이메일 배포 목록을 사용하십시오. 이메일 배포 목록을 사용하면 조직 내 개인이 오고 가더라도 소유권과 접근성을 유지할 수 있습니다. 청구, 운영 및 보안 알림을 위한 대체 연락처를 설정하고 그에 따라 적절한 이메일 배포 목록을 사용하세요. AWS 이 이메일 주소를 사용하여 사용자에게 연락하므로 계속 액세스할 수 있어야 합니다.

계정 이름, 루트 사용자 암호 또는 루트 사용자 이메일 주소를 편집하려면

1. https://console.aws.amazon.com/billing/home?#/account에서 과금 정보 및 비용 관리 콘솔의 계정 설정 페이지에 로그인합니다.
2. 계정 설정 페이지에서 계정 설정 옆의 편집을 선택합니다.
3. 업데이트하려는 필드 옆에서 편집을 선택합니다.
4. 변경을 입력한 후 변경 내용 저장을 선택합니다.
5. 변경을 모두 마치고 완료를 선택합니다.

연락처 정보를 편집하려면

1. 계정 설정 페이지의 연락처 정보에서 편집을 선택합니다.
2. 변경하려는 필드에 업데이트된 정보를 입력한 다음 업데이트를 선택합니다.

대체 연락처를 추가, 업데이트 또는 제거하려면

1. 계정 설정 페이지의 대체 연락처에서 편집을 선택합니다.
2. 변경하려는 필드에 업데이트된 정보를 입력한 다음 업데이트를 선택합니다.

ACCT.02 - 루트 사용자의 사용 제한

루트 사용자는 계정에 가입할 때 생성되며, 이 사용자는 AWS 계정에 대한 모든 소유권 및 변경할 수 없는 권한을 가집니다. 루트 사용자를 필요로 하는 작업에만 사용합니다. 자세한 내용은 루트 사용자 보안 인증이 필요한 작업(AWS Account Management)을 참조하세요. IAM 역할을 가진 페더레이션 사용자 등의 다른 유형의 IAM 자격 증명을 사용하여 계정에서 다른 모든 작업을 수행합니다. 자세한 내용은 AWS 보안 자격 증명(IAM 설명서)을 참조하세요.

루트 사용자의 사용 제한

1. ACCT.05 - 로그인하려면 다중 인증(MFA) 필요에 설명된 대로 루트 사용자에 대해 다중 인증(MFA)을 요구합니다.
2. 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다. 사용자 액세스 구성에 대한 자세한 내용은 ACCT.03 - 각 사용자에 대한 콘솔 액세스 구성 섹션을 참조하세요.

ACCT.03 - 각 사용자에 대한 콘솔 액세스 구성

가장 좋은 방법은 임시 자격 증명을 사용하여 리소스에 대한 액세스 권한을 부여하는 것입니다. AWS AWS 계정 임시 보안 인증은 수명이 제한되어 있어서, 더 이상 필요하지 않을 때 교체하거나 명시적으로 취소할 필요가 없습니다. 자세한 내용은 임시 보안 인증(IAM 설명서)을 참조하세요.

일반 사용자의 경우 AWS Okta, Active Directory 또는 Ping Identity와 같은 AWS IAM Identity Center중앙 집중식 ID 공급자 (IdP) 의 페더레이션 ID를 사용하는 것이 좋습니다. 사용자를 페더레이션하면 단일 중앙 위치에서 ID를 정의할 수 있으며 사용자는 단 하나의 자격 증명 세트를 사용하는 등 AWS여러 애플리케이션과 웹 사이트에 안전하게 인증할 수 있습니다. 자세한 내용은 IAM Identity Center (웹 사이트) 에서의 AWS ID 페더레이션을 참조하십시오.AWS

> **Note**
>
> ID 페더레이션은 단일 계정 아키텍처에서 다중 계정 아키텍처로 전환을 복잡하게 만들 수 있습니다. 스타트업은 AWS Organizations에서 관리되는 다중 계정 아키텍처를 구축할 때까지 ID 페더레이션 구현을 미루는 것이 일반적입니다.

ID 페더레이션을 설정하려면

1. IAM Identity Center를 사용하는 경우 Getting started(IAM Identity Center 설명서)를 참조하세요.

   외부 또는 타사 IdP를 사용하는 경우 IAM 자격 증명 공급자 생성(IAM 설명서)을 참조하세요.
2. IdP가 다중 인증(MFA)을 적용하는지 확인합니다.
3. ACC.04 - 권한 할당에 따라 권한을 적용합니다.

ID 페더레이션을 구성할 준비가 되지 않은 스타트업의 경우 IAM에서 직접 사용자를 생성할 수 있습니다. 이는 만료되지 않는 장기 보안 인증이므로 권장되는 보안 모범 사례는 아닙니다. 그러나 이는 초기 운영 중인 스타트업이 운영 준비가 되었을 때 다중 계정 아키텍처로 전환하는 데 어려움을 겪지 않도록 하기 위한 일반적인 방법입니다.

기본적으로 AWS Management Console에 액세스해야 하는 사람마다 IAM 사용자를 생성할 수 있습니다. IAM 사용자를 구성하는 경우 사용자 간에 보안 인증을 공유하지 말고 장기 보안 인증을 정기적으로 교체합니다.

> **Warning**
>
> IAM 사용자는 장기 자격 증명을 보유하므로 보안상 위험이 있습니다. 이 위험을 줄이려면 이러한 사용자에게 작업을 수행하는 데 필요한 권한만 제공하고 더 이상 필요하지 않을 경우 이러한 사용자를 제거하는 것이 좋습니다.

IAM 사용자 생성

1. IAM 사용자 생성(IAM 설명서).
2. ACC.04 - 권한 할당에 따라 권한을 적용합니다.

ACC.04 - 권한 할당

IAM 자격 증명(사용자 그룹 또는 역할)에 정책을 할당하여 계정의 사용자 권한을 구성합니다. 권한을 사용자 지정하거나 여러 일반 사용 사례에 권한을 제공하도록 설계된 독립 실행형 정책인 AWS 관리형 정책을 연결할 수 있습니다. AWS 권한을 사용자 지정하는 경우 최소 권한을 부여하는 보안 모범 사례를 따르세요. 최소 권한은 각 사용자에게 작업을 수행하는 데 필요한 최소 권한 세트를 부여하는 방법입니다.

페더레이션형 ID를 사용하는 경우 사용자는 외부 ID 제공업체를 통해 IAM 역할을 맡아 계정에 액세스합니다. IAM 역할은 조직의 IdP로 인증된 사용자가 수행할 수 있는 작업을 정의합니다. AWS이 역할에 사용자 지정 또는 AWS 관리형 정책을 적용하여 권한을 구성합니다.

페더레이션형 ID에 권한 할당

- IAM Identity Center를 사용하는 경우 Use IAM policies in permission sets(IAM Identity Center 설명서)를 참조하세요.

  외부 또는 타사 IdP를 사용하는 경우 IAM 자격 증명 권한 추가(IAM 설명서)를 참조하세요.

IAM 사용자를 사용하는 경우 사용자 그룹 또는 역할을 사용하여 여러 IAM 사용자의 권한을 관리할 수 있습니다. 사용자 그룹은 관리가 쉽고 잘못된 구성으로 사용자 계정에 보안 위험을 초래할 가능성이 적으므로 스타트업에는 사용자 그룹이 권장됩니다. 직무에 따라 사용자를 사용자 그룹에 지정합니다. 사용자 그룹의 예로는 애플리케이션, 데이터, 네트워킹, 개발 운영 (DevOps) 엔지니어 등이 있습니다. 또한 의사결정 권한에 따라 사용자 유형을 더 작은 사용자 그룹(예: 수석 또는 비수석 엔지니어)으로 나눌 수 있습니다.

IAM 사용자에 대한 권한을 할당

1. IAM 사용자 그룹을 생성합니다(IAM 설명서).
2. IAM 사용자 그룹에 AWS 관리형 정책을 연결합니다 (IAM 설명서).

ACCT.05 - 로그인하려면 다중 인증(MFA) 필요

MFA에는 인증 문제에 응답을 생성하는 디바이스가 있습니다. 로그인 과정을 완료하려면 각 사용자의 보안 인증과 디바이스에서 생성한 응답이 필요합니다. 보안 모범 사례로, 특히 계정 루트 사용자 및 IAM 사용자와 같은 장기 자격 증명의 경우 MFA를 AWS 계정 액세스용으로 활성화하십시오.

루트 사용자에 대해 MFA 설정

1. 에 로그인하십시오. AWS Management Console https://console.aws.amazon.com/
2. 탐색 모음의 오른쪽에서 계정 이름을 선택한 다음 내 보안 자격 증명을 선택합니다.
3. 필요한 경우 보안 인증으로 계속을 선택합니다.
4. 다중 인증(MFA) 섹션을 확장합니다.
5. Activate MFA(MFA 활성화)를 선택합니다.
6. 마법사의 지침에 따라 MFA 디바이스를 적절히 구성하세요. 자세한 내용은 Enabling MFA devices for users in AWS(IAM 설명서)를 참조하세요.

IAM Identity Center에서 MFA 설정

- MFA를 활성화합니다(IAM Identity Center 설명서).

IAM 사용자에 대해 MFA 설정

1. 로그인 보안 인증을 사용하여 https://console.aws.amazon.com/iam에서 IAM 콘솔에 로그인합니다.
2. 오른쪽 상단의 탐색 모음에서 사용자 이름을 선택한 다음 My Security Credentials(내 보안 인증)를 선택합니다.
3. AWS IAM 보안 인증(IAM credentials) 탭의 멀티 팩터 인증(Multi-factor authentication) 섹션에서 내 MFA 디바이스 관리(Manage MFA device)를 선택합니다.

다른 IAM 사용자에 대해 MFA 설정

1. 에서 AWS Management Console 로그인하고 IAM 콘솔을 엽니다. https://console.aws.amazon.com/iam
2. 탐색 창에서 사용자를 선택합니다.
3. MFA를 활성화하려는 사용자의 이름을 선택한 다음 Security credentials(보안 인증) 탭을 선택합니다.
4. Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.
5. 마법사의 지침에 따라 MFA 디바이스를 적절히 구성하세요. 자세한 내용은 Enabling MFA devices for users in AWS(IAM 설명서)를 참조하세요.

ACCT.06 - 암호 정책 적용

사용자는 로그인 자격 증명을 AWS Management Console 제공하여 에 로그인하며, MFA를 사용하는 것이 좋습니다. 무차별 대입 공격이나 소셜 엔지니어링을 통한 검색을 방지하려면 강력한 암호 정책을 준수하도록 합니다.

강력한 암호에 대한 최신 권장 사항에 대한 자세한 내용은 Center for Internet Security(CIS) 웹 사이트의 Password Policy Guide를 참조하세요.

IAM 사용자의 경우 사용자 지정 IAM 암호 정책에서 암호 요구 사항을 구성할 수 있습니다. 자세한 내용은 IAM 사용자의 계정 암호 정책 설정(IAM 설명서)을 참조하세요.

사용자 지정 암호 정책 생성

1. 에 AWS Management Console 로그인하고 에서 IAM 콘솔을 엽니다. https://console.aws.amazon.com/iam
2. 탐색 창에서 계정 설정(Account settings)를 선택합니다.
3. [암호 정책(Password policy)] 섹션에서 [암호 정책 변경(Change password policy)]을 선택합니다.
4. 암호 정책에 적용할 옵션을 선택하고 변경 사항 저장을 선택합니다.

ACCT.07 — 보호된 S3 버킷에 CloudTrail 로그를 전송합니다.

AWS 계정의 사용자, 역할, 서비스가 수행한 작업은 에 이벤트로 기록됩니다 AWS CloudTrail. CloudTrail 기본적으로 활성화되어 있으며 CloudTrail 콘솔에서 90일간의 이벤트 기록 정보에 액세스할

수 있습니다. AWS 인프라 전반의 계정 활동을 보고, 검색하고, 다운로드하고, 보관하고, 분석하고, 이에 대응하려면 이벤트 기록으로 CloudTrail 이벤트 보기 (CloudTrail 설명서) 를 참조하십시오.

CloudTrail 기록을 추가 데이터와 함께 90일 이상 보존하려면 모든 이벤트 유형에 대한 로그 파일을 Amazon Simple Storage Service (Amazon S3) 버킷으로 전송하는 새 트레일을 생성합니다. CloudTrail 콘솔에서 트레일을 생성하면 멀티 리전 트레일이 생성됩니다.

모든 사람의 로그를 S3 AWS 리전 버킷으로 전달하는 트레일을 만들려면

1. 트레일 생성 (CloudTrail 설명서). 로그 이벤트 선택 페이지에서 다음을 수행합니다.
   a. API 활동에서 읽기와 쓰기를 모두 선택합니다.
   b. 사전 프로덕션 환경에서 AWS KMS 이벤트 제외를 선택합니다. 이렇게 하면 모든 AWS Key Management Service (AWS KMS) 이벤트가 트레일에서 제외됩니다. AWS KMS `Encrypt`,`Decrypt`, 와 같은 읽기 액션은 대량의 이벤트를 생성할 `GenerateDataKey` 수 있습니다.

      프로덕션 환경의 경우 쓰기 관리 이벤트를 로깅하도록 선택하고 AWS KMS 이벤트 제외 확인란을 선택 취소합니다. 대용량 AWS KMS 읽기 이벤트는 제외되지만, `DisableDelete`, 같은 관련 쓰기 이벤트는 계속 기록합니다. `ScheduleKey` 프로덕션 환경에 권장되는 최소 AWS KMS 로깅 설정입니다.
2. [Trails] 페이지에 새 추적이 나타납니다. 약 15분 후에 계정에서 이루어진 API (AWS 애플리케이션 프로그래밍 인터페이스) 호출을 보여주는 로그 파일을 CloudTrail 게시합니다. 지정한 S3 버킷에서 로그 파일을 볼 수 있습니다.

로그 파일을 저장하는 CloudTrail S3 버킷을 보호하는 데 도움이 됩니다.

1. 로그 파일을 저장하는 모든 버킷에 대한 Amazon S3 버킷 정책 (CloudTrail 설명서) 을 검토하고 필요에 따라 조정하여 불필요한 액세스를 제거하십시오.
2. 보안 모범 사례로 반드시 `aws:SourceArn` 조건 키를 버킷 정책에 수동으로 추가합니다. 자세한 내용은 조직 트레일의 로그 파일을 저장하는 데 사용할 Amazon S3 버킷 생성 또는 업데이트 (CloudTrail 설명서) 를 참조하십시오.
3. MFA 삭제를 활성화합니다(Amazon S3 설명서).

ACCT.08 - 프라이빗 S3 버킷에 대한 퍼블릭 액세스 차단

기본적으로 의 루트 사용자와 IAM 보안 주체를 사용하는 경우 해당 보안 주체가 생성한 Amazon S3 버킷을 읽고 쓸 수 있는 권한이 있습니다. AWS 계정 ID 기반 정책을 사용하여 추가 IAM 보안 주체에 액세스 권한을 부여하고, 버킷 정책을 사용하여 액세스 조건을 적용할 수 있습니다. 퍼블릭 버킷에 대한 일반 퍼블릭 액세스 권한을 부여하는 버킷 정책을 생성할 수 있습니다.

2023년 4월 28일 이후에 생성된 버킷에는 퍼블릭 액세스 차단 설정이 기본적으로 활성화되어 있습니다. 이 날짜 이전에 생성된 버킷의 경우 사용자가 버킷 정책을 잘못 구성하여 의도치 않게 퍼블릭에 액세스 권한을 부여할 수 있습니다. 각 버킷에 대해 퍼블릭 액세스 차단 설정을 활성화하면 이러한 구성 오류를 방지할 수 있습니다. 퍼블릭 S3 버킷의 현재 또는 향후 사용 사례가 없는 경우 AWS 계정 레벨에서 이 설정을 활성화하십시오. 이 설정은 퍼블릭 액세스를 허용하는 정책을 방지합니다.

S3 버킷에 대한 퍼블릭 액세스 방지

- S3 버킷의 퍼블릭 액세스 차단 설정을 구성합니다(Amazon S3 설명서).

AWS Trusted Advisor 공개 목록 또는 읽기 액세스를 허용하는 S3 버킷에 대해 노란색 검색 결과를 생성하고, 공개 업로드 또는 삭제를 허용하는 버킷에 대해 빨간색 검색 결과를 생성합니다. 기준선으로 제어 ACCT.12 - Trusted Advisor를 사용하여 고위험 문제 모니터링 및 해결에 따라 잘못 구성된 버킷을 식별하고 수정합니다. 공개적으로 액세스 가능한 S3 버킷도 Amazon S3 콘솔에 표시됩니다.

ACT.09 - 사용하지 않는 VPC, 서브넷 및 보안 그룹 삭제

보안 문제가 발생할 가능성을 줄이려면 사용되지 않는 리소스를 삭제하거나 사용 중지합니다. 새 AWS 계정에서는 기본적으로 모든 AWS 리전계정에서 가상 사설 클라우드 (VPC) 가 자동으로 생성되므로 퍼블릭 서브넷에 공용 IP 주소를 할당할 수 있습니다. 그러나 이러한 VPC가 필요하지 않은 경우 리소스가 의도하지 않게 노출될 위험이 있습니다.

사용하지 않는 경우 워크로드를 배포할 수 있는 리전의 VPC뿐만 아니라 모든 리전의 기본 VPC를 삭제합니다. VPC를 삭제하면 서브넷 및 보안 그룹과 같은 구성 요소도 삭제됩니다.

> **Note**
>
> Amazon EC2 글로벌 뷰 콘솔(https://console.aws.amazon.com/ec2globalview/home)에서 모든 리전과 VPC를 볼 수 있습니다. 자세한 내용은 Amazon EC2 Global View를 사용하여 리전 간 리소스 나열 및 필터링(Amazon EC2 설명서)을 참조하세요.

사용하지 않는 기본 VPC 삭제

1. VPC를 삭제합니다(Amazon VPC 설명서).
2. 다른 리전의 VPC에 대해 필요에 따라 반복합니다.

ACCT.10 — 지출을 모니터링하도록 구성합니다 AWS Budgets .

AWS Budgets 비용이 목표 임계값을 초과할 것으로 예측되면 알림을 통해 월별 비용 및 사용량을 모니터링할 수 있습니다. 예상 비용 알림은 예상치 못한 활동을 알려주어 AWS Trusted Advisor Amazon과 같은 다른 모니터링 시스템 외에도 추가 방어 기능을 제공할 수 있습니다. GuardDuty AWS 비용을 모니터링하고 파악하는 것도 운영 위생의 일부입니다.

에 예산을 세우려면 AWS Budgets

- 비용 예산 (AWS Budgets 문서) 을 만드세요.

ACCT.11 — 알림 활성화 및 알림 응답 GuardDuty

GuardDuty Amazon은 악의적 또는 무단 행동을 지속적으로 모니터링하여 AWS 계정, 워크로드 및 데이터를 보호하는 위협 탐지 서비스입니다. 예상치 못한 잠재적 악의적 활동을 탐지하면 가시성과 해결을 위한 상세한 보안 결과를 GuardDuty 제공합니다. GuardDuty 암호화폐 채굴 활동, Tor 클라이언트 및 릴레이로부터의 액세스, 예상치 못한 행동, 손상된 IAM 자격 증명과 같은 위협을 탐지할 수 있습니다. 탐지 결과를 GuardDuty 활성화하고 이에 대응하여 사용자 환경에서 잠재적으로 악의적이거나 승인되지 않은 행동을 차단하세요. AWS 의 GuardDuty 결과에 대한 자세한 내용은 검색 유형 (GuardDuty 설명서) 을 참조하십시오.

Amazon CloudWatch Events를 사용하여 검색 결과 GuardDuty 생성 또는 검색 결과 변경 시 자동 알림을 설정할 수 있습니다. 먼저 Amazon Simple Notification Service(SNS) 주제를 설정하고 주제에 엔드포인트 또는 이메일 주소를 추가합니다. 그런 다음 GuardDuty 검색 결과를 위한 CloudWatch 이벤트를 설정하면 이벤트 규칙이 Amazon SNS 주제의 엔드포인트에 알립니다.

활성화 및 알림 GuardDuty GuardDuty

1. Amazon GuardDuty (GuardDuty 설명서) 을 활성화합니다.
2. GuardDuty 결과를 알려주는 CloudWatch 이벤트 규칙을 생성하십시오 (GuardDuty설명서).

ACCT.12 - Trusted Advisor를 사용하여 고위험 문제 모니터링 및 해결

AWS Trusted Advisor AWS 인프라를 수동적으로 스캔하여 보안, 성능, 비용 및 안정성과 관련된 위험도가 높거나 영향이 큰 문제가 있는지 확인합니다. 그런 다음 영향을 받는 리소스에 대한 자세한 정보와 수정 권장 사항을 제공합니다. 검사 및 설명의 전체 목록은 AWS Trusted Advisor 검사 참조 (문서)를 참조하십시오.Trusted Advisor

정기적으로 Trusted Advisor 결과를 검토하고 필요에 따라 문제를 수정하십시오. AWS 비즈니스 지원 또는 Enterprise Support 플랜을 사용하는 경우 주간 조사 결과 이메일을 구독할 수 있습니다. 자세한 내용은 Set up notification preferences(AWS Support 설명서를 참조하세요.

문제를 보려면 다음을 참조하십시오. Trusted Advisor

- 검사 범주 보기 (AWS Support 문서) 의 지침에 따라 각 검사 범주를 검토하십시오. 최소한 빨간색으로 표시된 조치 권장 문제를 검토하는 것이 좋습니다.

워크로드 보안

이 섹션의 제어 및 권장 사항은 워크로드를 구축하는 동안 AWS에서 실행되는 워크로드를 보호하는 데 도움이 됩니다. 애플리케이션 시크릿과 액세스 범위를 관리하고, 개인 리소스에 대한 액세스 경로를 최소화하고, 암호화를 사용하여 전송 중 데이터와 저장 데이터를 보호하는 보안 방식을 중점적으로 다룹니다.

이 섹션은 다음 주제를 포함합니다.

WKLD.01 - 컴퓨팅 환경 권한에 IAM 역할 사용

AWS Identity and Access Management(IAM)에서 역할은 구성 가능한 기간 동안 사람이나 서비스가 맡을 수 있는 권한 세트를 나타냅니다. 역할을 사용하면 장기 보안 인증을 저장하거나 관리할 필요가 없으므로 의도하지 않은 사용 가능성이 크게 줄어듭니다. 지원되는 경우 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS Fargate 작업 및 서비스, AWS Lambda 함수 및 기타 AWS 컴퓨팅 서비스에 IAM 역할을 직접 할당합니다. AWS SDK를 사용하고 이러한 컴퓨팅 환경에서 실행되는 애플리케이션은 인증을 위해 자동으로 IAM 역할 보안 인증을 사용합니다.

각 서비스에 대한 IAM 역할 사용에 대한 접근 방식과 지침은 해당 서비스에 대한 AWS 설명서에서 확인할 수 있습니다. 예를 들어, 다음을 참조하세요.

- Amazon EC2의 IAM 역할(Amazon EC2 설명서)
- IAM roles for tasks(Amazon Elastic Container Service 설명서)
- Lambda 실행 역할(Lambda 설명서)

WKLD.02 - 리소스 기반 정책 권한으로 보안 인증 사용 범위 제한

정책은 권한을 정의하거나 액세스 조건을 지정할 수 있는 객체입니다. 정책에는 두 가지 기본 유형이 있습니다.

- ID 기반 정책은 보안 주체에 연결되며 AWS 환경에서 보안 주체의 권한을 정의합니다.
- 리소스 기반 정책은 Amazon Simple Storage Service(S3) 버킷, Virtual Private Cloud(VPC) 엔드포인트 등의 리소스에 연결됩니다. 이 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

보안 주체가 리소스에 대해 작업을 수행할 수 있는 액세스를 허용하려면 ID 기반 정책에서 권한을 부여받아야 하며 리소스 기반 정책의 조건을 충족해야 합니다. 자세한 내용은 자격 증명 기반 정책 및 리소스 기반 정책(IAM 설명서)을 참조하세요.

리소스 기반 정책의 권장 조건은 다음과 같습니다.

- `aws:PrincipalOrgID` 조건을 사용하여 지정된 조직(AWS Organizations에 정의됨)의 보안 주체로만 액세스를 제한합니다.
- `aws:SourceVpc` 또는 `aws:SourceVpce` 조건을 각각 사용하여 특정 VPC 또는 VPC 엔드포인트에서 발생하는 트래픽에 대한 액세스를 제한합니다.
- `aws:SourceIp` 조건을 사용하여 소스 IP 주소를 기반으로 트래픽을 허용하거나 거부합니다.

다음은 `aws:PrincipalOrgID` 조건을 사용하여 **<o-xxxxxxxxxxx>** 조직의 보안 주체만 **<bucket-name>** S3 버킷에 액세스하도록 허용하는 리소스 기반 정책의 예입니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
```

```
        "Effect":"Allow",
        "Principal":"*",
        "Action":"s3:*",
        "Resource":"arn:aws:s3:::<bucket-name>/*",
        "Condition": {
          "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
        }
      }
   ]
}
```

WKLD.03 - 임시 시크릿 또는 시크릿 관리 서비스 사용

애플리케이션 시크릿은 주로 키 페어, 액세스 토큰, 디지털 인증서, 로그인 보안 인증과 같은 보안 인증 정보로 구성됩니다. 애플리케이션은 이러한 시크릿을 사용하여 데이터베이스와 같이 애플리케이션이 의존하는 다른 서비스에 대한 액세스 권한을 얻습니다. 이러한 시크릿을 보호하려면 임시 시크릿(요청 시 생성되고 IAM 역할과 같이 수명이 짧음)이거나 시크릿 관리 서비스에서 검색하는 것이 좋습니다. 이렇게 하면 정적 구성 파일에 보관과 같이 덜 안전한 메커니즘을 통한 우발적인 노출을 방지할 수 있습니다. 또한 애플리케이션 코드를 개발 환경에서 프로덕션 환경으로 쉽게 승격시킬 수 있습니다.

시크릿 관리 서비스의 경우 AWS Systems Manager의 기능인 Parameter Store와 AWS Secrets Manager를 조합하여 사용하는 것이 좋습니다.

- Parameter Store를 사용하여 전체 길이가 짧고 자주 액세스하는 문자열 기반의 개별 키-값 페어인 시크릿과 기타 파라미터를 관리합니다. AWS Key Management Service(AWS KMS) 키를 사용하여 시크릿을 암호화합니다. Parameter Store의 표준 계층에 파라미터를 저장하는 데는 요금이 부과되지 않습니다. 파라미터 티어에 대한 자세한 내용은 Managing parameter tiers(Systems Manager 설명서)를 참조하세요.
- Secrets Manager를 사용하여 문서 형식(예: 여러 관련 키-값 페어)이거나 4KB보다 크거나(예: 디지털 인증서) 자동 교체의 이점을 얻을 수 있는 보안 시크릿을 저장합니다.

Parameter Store API를 사용하여 Secrets Manager에 저장된 시크릿을 검색할 수 있습니다. 이렇게 하면 두 서비스를 함께 사용할 때 애플리케이션의 코드를 표준화할 수 있습니다.

Parameter Store에서 시크릿 관리

1. 대칭 AWS KMS 키를 생성합니다(AWS KMS 설명서).
2. SecureString 파라미터를 생성합니다(Systems Manager 설명서). Parameter Store의 시크릿은 `SecureString` 데이터 유형을 사용합니다.

3. 애플리케이션에서 프로그래밍 언어에 맞는 AWS SDK를 사용하여 Parameter Store에서 파라미터를 검색합니다. Java의 예는 GetParameter.java(AWS 코드 샘플 카탈로그)를 참조하세요.

Secrets Manager에서 시크릿 관리

1. 시크릿을 생성합니다(Secrets Manager 설명서).
2. 코드로 AWS Secrets Manager에서 시크릿을 검색합니다(Secrets Manager 설명서).

   Use AWS Secrets Manager client-side caching libraries to improve the availability and latency of using your secrets(AWS 블로그 게시물)를 읽는 것이 중요합니다. 이미 모범 사례가 구현된 클라이언트측 SDK를 사용하면 Secrets Manager의 사용 및 통합이 가속화되고 단순화됩니다.

WKLD.04 - 애플리케이션 시크릿 노출 방지

로컬 개발 중에는 애플리케이션 스크릿이 로컬 구성 또는 코드 파일에 저장되어 실수로 소스 코드 리포지토리에 체크인될 수 있습니다. 공공 서비스 제공업체에 호스팅된 보안되지 않은 리포지토리는 무단 액세스가 발생하고 이후 이러한 시크릿이 검색될 수 있습니다. 사용 가능한 도구를 사용하여 시크릿이 체크인되지 않도록 합니다. 수동 코드 검토 프로세스의 일부로 노출된 시크릿에 대한 검사를 통합하세요.

애플리케이션 시크릿이 소스 코드 리포지토리에 체크인되는 것을 방지할 수 있는 몇 가지 일반적인 도구는 다음과 같습니다.

- Gitleaks(GitHub 리포지토리)
- Whispers(GitHub 리포지토리)
- detect-secrets(GitHub 리포지토리)
- git-secrets(GitHub 리포지토리)
- TruffleHog(GitHub 리포지토리)

WKLD.05 - 노출된 시크릿 탐지 및 해결

WKLD.03 - 임시 시크릿 또는 시크릿 관리 서비스 사용과 WKLD.04 - 애플리케이션 시크릿 노출 방지에서 시크릿을 보호하기 위한 조치를 취합니다. 이 제어를 통해 시크릿이 이러한 예방 조치를 우회했는지 여부를 탐지할 수 있는 솔루션을 배포하고 그에 따라 수정할 수 있습니다.

Amazon CodeGuru Reviewer는 소스 코드에서 애플리케이션 시크릿을 탐지하고 탐지된 시크릿을 수정하여 Secrets Manager에 게시하는 메커니즘을 제공합니다. Secrets Manager에서 시크릿을 검색하기 위한 애플리케이션 코드도 제공됩니다. 비용-편익 분석을 수행하여 이 솔루션이 비즈니스에 적합한지 결정합니다. 대안으로 WKLD.04 - 애플리케이션 시크릿 노출 방지의 일부 오픈 소스 솔루션은 기존 시크릿에 대한 탐지 기능을 제공합니다.

Secrets Manager와 CodeGuru Reviewer 통합 설정

- 하드코딩된 시크릿을 CodeGuru Reviewer로 식별하고 AWS Secrets Manager로 보호합니다(AWS 블로그 게시물 및 안내 연습).

WKLD.06 - SSH 또는 RDP 대신 Systems Manager 사용

인터넷 게이트웨이를 가리키는 기본 경로가 있는 퍼블릭 서브넷은 인터넷 경로가 없는 프라이빗 서브넷보다 본질적으로 보안 위험이 더 큽니다. 프라이빗 서브넷에서 EC2 인스턴스를 실행하고 AWS Systems Manager의 Session Manager 기능을 사용하여 AWS Command Line Interface(AWS CLI) 또는 AWS Management Console을 통해 인스턴스에 원격으로 액세스할 수 있습니다. 그런 다음 AWS CLI 또는 콘솔을 사용하여 보안 터널을 통해 인스턴스에 연결하는 세션을 시작할 수 있으므로 Secure Shell(SSH) 또는 Windows 원격 데스크톱 프로토콜(RDP)에 사용되는 추가 보안 인증을 관리할 필요가 없습니다.

퍼블릭 서브넷에서 EC2 인스턴스를 실행하거나, 점프 박스를 실행하거나, Bastion Host를 실행하는 대신 Session Manager를 사용합니다.

Session Manager 설정

1. EC2 인스턴스가 Amazon Linux 2 또는 Ubuntu와 같은 최신 운영 체제 Amazon Machine Image(AMI)를 사용하고 있는지 확인합니다. AWS Systems Manager Agent(SSM Agent)는 AMI에 사전 설치되어 있습니다.
2. 인스턴스가 인터넷 게이트웨이나 VPC 엔드포인트를 통해 다음 주소에 연결되어 있는지 확인합니다(**<region>**을 적절한 AWS 리전으로 바꿈).
    a. Ec2messages.<region>.amazonaws.com
    b. ssm.<region>.amazonaws.com
    c. ssmmessages.<region>.amazonaws.com
3. AWS 관리형 정책 `AmazonSSMManagedInstanceCore`를 인스턴스에 연결된 IAM 역할에 연결합니다.

자세한 내용은 Session Manager 설정(Systems Manager 설명서)을 참조하세요.

세션 시작

- 세션 시작(Systems Manager 설명서)

WKLD.07 - 민감한 데이터가 포함된 S3 버킷에 대한 데이터 이벤트 로깅

기본적으로 AWS CloudTrail은 관리 이벤트, 즉 계정에서 리소스를 생성, 수정 또는 삭제하는 이벤트를 캡처합니다. 이러한 관리 이벤트는 Amazon Simple Storage Service 버킷의 개별 객체에 대한 읽기 또는 쓰기 작업을 캡처하지 않습니다. 보안 이벤트 중 개별 레코드 또는 객체 수준에서 무단 데이터 액세스나 사용을 캡처하는 것이 중요합니다. CloudTrail을 사용하여 탐지 및 감사 목적으로 민감하거나 비즈니스에 중요한 데이터를 저장하는 S3 버킷에 대한 데이터 이벤트를 로깅합니다.

> **Note**
>
> 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

트레일에 대한 데이터 이벤트 로깅

1. AWS Management Console에 로그인한 다음 https://console.aws.amazon.com/cloudtrail/에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 [추적(Trails)]을 선택한 다음, 추적 이름을 선택합니다.
3. 일반 세부 정보에서 편집을 선택하여 다음 설정을 변경합니다. 추적 이름은 변경할 수 없습니다.
    a. 데이터 이벤트에서 편집을 선택합니다.
    b. [데이터 이벤트 소스(Data event source)]에서 S3를 선택합니다.
    c. 현재 및 향후의 모든 S3 버킷에서 읽기 및 쓰기를 선택 취소합니다.
    d. 개별 버킷 선택에서 데이터 이벤트를 로깅할 버킷을 찾습니다. 이 창에서 여러 버킷을 선택할 수 있습니다. 더 많은 버킷의 데이터 이벤트를 로그하려면 [버킷 추가(Add bucket)]를 선택합니다. [읽기(Read)] 이벤트(예:`GetObject`), [쓰기(Write)] 이벤트(예:`PutObject`) 또는 둘 다를 로그하도록 선택합니다.
    e. [추적 업데이트(Update trail)]를 선택합니다.

WKLD.08 - Amazon EBS 볼륨 암호화

AWS 계정의 기본 동작으로 Amazon Elastic Block Store(Amazon EBS) 볼륨의 암호화를 적용합니다. 암호화된 볼륨은 지연 시간에 미치는 영향을 최소화하면서 암호화되지 않은 볼륨과 동일한 초당 입출력 작업 처리량(IOPS) 성능을 가집니다. 이렇게 하면 규정 준수 또는 기타 이유로 나중에 볼륨을 재구축할 수 없습니다. 자세한 내용은 Must-know best practices for Amazon EBS encryption(AWS 블로그 게시물)을 참조하세요.

Amazon EBS 볼륨 암호화

- 암호화를 기본적으로 활성화합니다(Amazon EC2 설명서).

WKLD.09 - Amazon RDS 데이터베이스 암호화

WKLD.08 - Amazon EBS 볼륨 암호화와 유사하게 Amazon Relational Database Service(RDS) 데이터베이스의 암호화를 활성화합니다. 이 암호화는 기본 볼륨 수준에서 수행되며 지연 시간에 미치는 영향을 최소화하면서 암호화되지 않은 볼륨과 동일한 IOPS 성능을 제공합니다. 자세한 내용은 Amazon RDS 리소스 암호화 개요(Amazon RDS 설명서)를 참조하세요.

RDS 데이터베이스 인스턴스 암호화

- 데이터베이스 인스턴스를 암호화합니다(Amazon RDS 설명서).

WKLD.10 - 프라이빗 서브넷에 프라이빗 리소스 배포

EC2 인스턴스, 데이터베이스, 대기열, 캐싱 또는 기타 인프라와 같이 직접 인터넷 액세스가 필요하지 않은 리소스를 VPC 프라이빗 서브넷에 배포합니다. 프라이빗 서브넷은 연결된 인터넷 게이트웨이로 향하는 경로가 라우팅 테이블에 선언되어 있지 않으므로 인터넷 트래픽을 수신할 수 없습니다. 인터넷으로 향하는 프라이빗 서브넷에서 시작되는 트래픽은 관리형 AWS NAT 게이트웨이 또는 퍼블릭 서브넷에서 NAT 프로세스를 실행하는 EC2 인스턴스를 통해 Network Address Translation(NAT)을 거쳐야 합니다. 네트워크 격리에 대한 자세한 내용은 Amazon VPC의 인프라 보안(Amazon VPC 설명서)를 참조하세요.

프라이빗 리소스 및 서브넷을 생성할 때는 다음 방법을 사용하세요.

- 프라이빗 서브넷을 생성할 때 퍼블릭 IPv4 주소 자동 할당을 비활성화합니다.

- 프라이빗 EC2 인스턴스를 생성할 때 퍼블릭 IP 자동 할당을 비활성화합니다. 이렇게 하면 잘못된 구성으로 인해 인스턴스가 실수로 퍼블릭 서브넷에 배포되는 경우 퍼블릭 IP가 할당되는 것을 막을 수 있습니다.

필요한 경우 구성의 일부로 리소스의 서브넷을 지정합니다. 확장 가능한 모듈식 VPC 아키텍처 빠른 시작(AWS Quick Starts)을 사용하여 모범 사례를 따르는 VPC를 배포할 수 있습니다.

WKLD.11 - 보안 그룹을 사용하여 네트워크 액세스 제한

보안 그룹을 사용하여 EC2 인스턴스, RDS 데이터베이스 및 기타 지원되는 리소스에 대한 트래픽을 제어합니다. 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용하는 규칙을 일관되게 정의하기 위해 모든 관련 리소스 그룹에 적용할 수 있는 가상 방화벽 역할을 합니다. IP 주소 및 포트를 기반으로 하는 규칙 외에도 보안 그룹은 다른 보안 그룹과 관련된 리소스의 트래픽을 허용하는 규칙을 지원합니다. 예를 들어, 데이터베이스 보안 그룹에 애플리케이션 서버 보안 그룹의 트래픽만 허용하는 규칙이 있을 수 있습니다.

기본적으로 보안 그룹은 모든 아웃바운드 트래픽을 허용하지만 인바운드 트래픽은 허용하지 않습니다. 아웃바운드 트래픽 규칙을 제거하거나, 아웃바운드 트래픽을 제한하고 인바운드 트래픽을 허용하도록 추가 규칙을 구성할 수 있습니다. 보안 그룹에 아웃바운드 규칙이 없는 경우 인스턴스에서 시작하는 아웃바운드 트래픽이 허용되지 않습니다. 자세한 내용은 보안 그룹을 사용하여 리소스에 대한 트래픽 제어(Amazon VPC 설명서)를 참조하세요.

다음 예에서는 Application Load Balancer에서 Amazon RDS for MySQL 데이터베이스에 연결되는 EC2 인스턴스로의 트래픽을 제어하는 3개의 보안 그룹이 있습니다.

보안 그룹	인바운드 규칙	아웃바운드 규칙
Application Load Balancer 보안 그룹	설명: 어디에서 들어오든 HTTPS 트래픽 허용 유형: HTTPS 소스: Anywhere-IPv4(0.0.0.0/0)	설명: 대상에 관계없이 모든 트래픽 허용 유형:: 모든 트래픽 대상: Anywhere-IPv4(0.0.0.0/0)
EC2 인스턴스 보안 그룹	설명: Application Load Balancer의 HTTP 트래픽 허용 유형: HTTP	설명: 대상에 관계없이 모든 트래픽 허용 유형:: 모든 트래픽

보안 그룹	인바운드 규칙	아웃바운드 규칙
	소스: Application Load Balancer 보안 그룹	대상: Anywhere-IPv4(0.0.0.0/0)
RDS 데이터베이스 보안 그룹	설명: EC2 인스턴스의 MySQL 트래픽 허용 유형: MySQL 소스: EC2 인스턴스 보안 그룹	아웃바운드 규칙 없음

WKLD.12 - VPC 엔드포인트를 사용하여 지원되는 서비스에 액세스

VPC에서 AWS 또는 기타 외부 서비스에 액세스해야 하는 리소스에는 인터넷(`0.0.0.0/0`) 또는 대상 서비스의 퍼블릭 IP 주소에 대한 라우팅이 필요합니다. VPC 엔드포인트를 사용하면 VPC에서 지원되는 AWS 또는 기타 서비스로의 프라이빗 IP 라우팅을 활성화할 수 있으므로 인터넷 게이트웨이, NAT 디바이스, 가상 프라이빗 네트워크(VPN) 연결 또는 AWS Direct Connect 연결을 사용할 필요가 없습니다.

VPC 엔드포인트는 서비스에 대한 액세스를 추가로 제어할 수 있도록 정책 및 보안 그룹 연결을 지원합니다. 예를 들어, Amazon DynamoDB에 대한 VPC 엔드포인트 정책을 작성하여 자체 권한 정책에 관계없이 항목 수준 작업만 허용하고 VPC의 모든 리소스에 대한 테이블 수준 작업은 금지할 수 있습니다. 특정 VPC 엔드포인트에서 시작된 요청만 허용하고 다른 모든 외부 액세스는 거부하도록 S3 버킷 정책을 작성할 수도 있습니다. 예를 들어, VPC 엔드포인트에는웹 애플리케이션의 비즈니스 로직 티어와 같은 애플리케이션별 보안 그룹에 연결된 EC2 인스턴스로만 액세스를 제한하는 보안 그룹 규칙이 있을 수 있습니다.

VPC 엔드포인트에는 여러 종류가 있습니다. VPC 인터페이스 엔드포인트를 사용하여 대부분의 서비스에 액세스합니다. DynamoDB는 게이트웨이 엔드포인트를 사용하여 액세스합니다. Amazon S3는 인터페이스 엔드포인트와 게이트웨이 엔드포인트를 모두 지원합니다. 단일 AWS 계정 및 리전 내에 포함된 워크로드에는 게이트웨이 엔드포인트가 권장되며 추가 비용이 발생하지 않습니다. 다른 VPC, 온프레미스 네트워크 또는 다른 AWS 리전의 S3 버킷과 같이 더 확장 가능한 액세스가 필요한 경우 인터페이스 엔드포인트가 권장됩니다. 인터페이스 엔드포인트에는 시간당 가동 시간 요금과 GB당 데이터 처리 요금이 발생하며, 두 요금 모두 AWS NAT 게이트웨이를 통해 `0.0.0.0/0`으로 데이터를 전송하는 데 드는 요금보다 낮습니다.

VPC 엔드포인트 사용에 대한 자세한 내용은 다음 리소스를 참조하세요.

- Amazon S3의 게이트웨이 엔드포인트와 인터페이스 엔드포인트 중에서 선택하는 방법에 대한 자세한 내용은 Choosing Your VPC Endpoint Strategy for Amazon S3(AWS 블로그 게시물)를 참조하세요.
- 인터페이스 엔드포인트 생성(Amazon VPC 설명서).
- 게이트웨이 엔드포인트를 생성합니다(Amazon VPC 설명서).
- 특정 VPC 또는 VPC 엔드포인트에 대한 액세스를 제한하는 S3 버킷 정책의 예는 특정 VPC에 대한 액세스 제한(Amazon S3 설명서)을 참조하세요.
- 예를 들어 작업을 제한하는 DynamoDB 엔드포인트 정책의 예는 Amazon DynamoDB에 대한 게이트웨이 엔드포인트(Amazon VPC 설명서)을 참조하세요.

WKLD.13 - 모든 퍼블릭 웹 엔드포인트에는 HTTPS 요구

HTTPS를 요구하여 웹 엔드포인트의 신뢰성을 높이고, 엔드포인트가 인증서를 사용하여 ID를 증명할 수 있도록 하고, 엔드포인트와 연결된 클라이언트 간의 모든 트래픽이 암호화되었는지 확인합니다. 퍼블릭 웹 사이트의 경우 검색 엔진 순위가 높아지는 추가 이점이 있습니다.

AWS Elastic Beanstalk, Amazon CloudFront, Amazon API Gateway, Elastic Load Balancing, AWS Amplify 등의 많은 AWS 서비스에서 리소스에 대한 퍼블릭 웹 엔드포인트를 제공합니다. 각 서비스에 HTTPS를 요구하는 방법에 대한 지침은 다음을 참조하세요.

- Elastic Beanstalk(Elastic Beanstalk 설명서)
- CloudFront(CloudFront 설명서)
- Application Load Balancer(AWS 지식 센터)
- Classic Load Balancer(AWS 지식 센터)
- Amplify(Amplify 설명서)

Amazon S3에 호스팅된 정적 웹 사이트는 HTTPS를 지원하지 않습니다. 이러한 웹 사이트에 HTTPS를 요구하려면 CloudFront를 사용합니다. CloudFront를 통해 콘텐츠를 제공하는 S3 버킷에 대한 퍼블릭 액세스는 필요하지 않습니다.

CloudFront를 사용하여 Amazon S3에서 호스팅되는 정적 웹 사이트 제공

1. CloudFront를 사용하여 Amazon S3에 호스팅된 정적 웹 사이트를 제공합니다(AWS 지식 센터).
2. 퍼블릭 S3 버킷에 대한 액세스를 구성하는 경우 최종 사용자와 CloudFront 간에 HTTPS가 필요합니다(CloudFront 설명서).

프라이빗 S3 버킷에 대한 액세스를 구성하는 경우 오리진 액세스 ID를 사용하여 Amazon S3 콘텐츠에 대한 액세스를 제한합니다(CloudFront 설명서).

또한 이전 프로토콜과의 호환성이 필요한 경우가 아니면 최신 전송 계층 보안(TLS) 프로토콜 및 암호를 요구하도록 HTTPS 엔드포인트를 구성합니다. 예를 들어, 기본 `ELBSecurityPolicy-2016-08` 대신 `ELBSecurityPolicy-FS-1-2-Res-2020-10` 또는 Application Load Balancer HTTPS 리스너에 사용 가능한 최신 정책을 사용합니다. 최신 정책에서는 최소 TLS 1.2, 전방향 보안, 최신 웹 브라우저와 호환되는 강력한 암호를 요구합니다.

HTTPS 퍼블릭 엔드포인트에 사용 가능한 보안 정책에 대한 자세한 내용은 다음을 참조하세요.

- Predefined SSL security policies for Classic Load Balancers(Elastic Load Balancing 설명서)
- Application Load Balancer의 보안 정책(Elastic Load Balancing 설명서)
- 최종 사용자와 CloudFront 간에 지원되는 프로토콜 및 암호(CloudFront 설명서)

WKLD.14 - 퍼블릭 엔드포인트에 엣지 보호 서비스 사용

EC2 인스턴스 또는 컨테이너와 같은 컴퓨팅 서비스에서 직접 트래픽을 처리하는 대신 엣지 보호 서비스를 사용합니다. 이는 인터넷의 수신 트래픽과 해당 트래픽을 처리하는 리소스 사이에 추가 보안 계층을 제공합니다. 이러한 서비스는 트래픽이 내부 리소스에 도달하기 전에 원치 않는 트래픽을 필터링하고, 암호화를 적용하고, 라우팅 또는 기타 규칙(예: 부하 분산)을 적용할 수 있습니다.

퍼블릭 엔드포인트 보호를 제공할 수 있는 AWS 서비스에는 AWS WAF, CloudFront, Elastic Load Balancing, API Gateway 및 Amplify Hosting이 포함됩니다. Elastic Load Balancing과 같은 VPC 기반 서비스를 퍼블릭 서브넷에서 프라이빗 서브넷에서 실행되는 웹 서비스 리소스에 대한 프록시로 실행합니다.

CloudFront, API Gateway 및 Amazon Route 53은 계층 3 및 4 분산 서비스 거부(DDoS) 공격으로부터 무료로 보호를 제공하며, AWS WAF는 계층 7 공격으로부터 보호할 수 있습니다.

각 서비스를 시작하기 위한 지침은 다음에서 확인할 수 있습니다.

- AWS WAF 시작하기(AWS 웹 사이트)
- Amazon CloudFront 시작하기(CloudFront 설명서)
- Elastic Load Balancing 시작하기(Elastic Load Balancing 설명서)
- API Gateway 시작하기(API Gateway 설명서)

- Getting started with Amplify Hosting(Amplify 설명서)

WKLD.15 - 템플릿에서 보안 제어 정의 및 CI/CD 방식으로 배포

코드형 인프라(IaC)는 소프트웨어 애플리케이션을 배포하는 데 사용되는 것과 동일한 파이프라인인 CI/CD(지속적 통합 및 지속적 전달) 파이프라인을 사용하여 배포하는 템플릿과 코드에 모든 AWS 서비스 리소스와 구성을 정의하는 방식입니다. AWS CloudFormation과 같은 IaC 서비스는 IAM ID 기반 정책과 리소스 기반 정책을 모두 지원하고 Amazon GuardDuty, AWS WAF, Amazon VPC 등의 AWS 보안 서비스를 지원합니다. 이러한 아티팩트를 IaC 템플릿으로 캡처하고 템플릿을 소스 코드 리포지토리에 커밋한 다음 CI/CD 파이프라인을 사용하여 배포합니다.

달리 필요한 경우가 아니면 동일한 리포지토리의 애플리케이션 코드를 사용하여 애플리케이션 권한 정책을 커밋하고, 일반 리소스 정책 및 보안 서비스 구성을 별도의 코드 리포지토리와 배포 파이프라인에서 관리합니다.

AWS에서 IaC 시작하기에 대한 자세한 내용은 AWS Cloud Development Kit (AWS CDK) 설명서를 참조하세요.

기여자

다음은 이 문서의 기여자입니다.

- Jay Michael, Principal Solutions Architect
- Cole Calistra, Principal Solutions Architect
- Justin Plock, Principal Solutions Architect
- Faisal Farooq, Solutions Architect
- Michael Nguyen, Sr. Solutions Architect
- Ritik Khatwani, Sr. Solutions Architect
- Paul Hawkins, Principal, CISO(Office of the Chief Information Security Officer)

지침과 검토에도 도움을 주신 다음 분들께 특별히 감사드립니다.

- Robert Put
- Mike Sullivan
- Bob Lee III

문서 기록

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

변경 사항	설명	날짜
Amazon S3 버킷 설정	2023년 4월 28일 이후에 생성된 Amazon S3 버킷에는 퍼블릭 액세스 차단 설정이 기본적으로 활성화되어 있음을 반영하기 위해 ACCT.08 – 프라이빗 S3 버킷에 대한 퍼블릭 액세스 방지 섹션을 업데이트했습니다.	2023년 5월 18일
IAM 보안 모범 사례	최신 AWS Identity and Access Management(IAM) 모범 사례에 맞춰 이 가이드를 업데이트했습니다. 자세한 내용은 IAM 설명서의 보안 모범 사례를 참조하세요.	2023년 2월 1일
IAM 역할	WKLD.01 – 컴퓨팅 환경 권한을 위한 IAM 역할 사용 섹션에 AWS 서비스 설명서에 대한 링크를 추가했습니다.	2022년 9월 22일
암호 정책	Center for Internet Security(CIS)의 최신 지침을 사용하도록 강력한 암호에 대한 권장 사항을 업데이트했습니다.	2022년 5월 10일
최초 게시	—	2022년 4월 13일

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.
- 리플랫포밍(리프트 앤드 리셰이프) - 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 숍) - 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.
- 재배치(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 재배치합니다.
- 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 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 및 등이 `SUM` 있습니다. `MAX`

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 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 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 가이드를 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 사이트와 AWS CAF 백서를 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 graph를 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 책인가요, 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 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 실행AWS의 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 엑설런스를 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 게시물을 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 구축을 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 가이드를 참조하세요.

CMDB

구성 관리 데이터베이스를 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 packs를 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 참조하세요. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 지속적 전달(Continuous Delivery)과 지속적인 개발을 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 분류를 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 구축을 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 서비스를 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 controls를 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 워크로로드의 재해 복구: 클라우드에서의 재해 복구를 참조하세요.

DML

데이터베이스 조작 언어를 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 방법을 참조하세요.

DR

재해 복구를 참조하십시오.

드리프트 감지

기준 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 매핑을 참조하십시오.

E

EDA

탐색적 데이터 분석을 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 생성을 참조하세요.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service(AWS KMS) 설명서의 Envelope encryption을 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 가이드를 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 영역AWS 리전, 컨트롤 플레인 또는 데이터 플레인과 같은 경계 AWS 클라우드 자세한 내용은 [AWS장애 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 그레디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 [다음을 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 제어를](#) 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 제한을 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 제한을 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 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, 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 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.

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. 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 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 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 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 구축을 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 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 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 AWS를 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 가이드를 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 environment를 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 적용을 참조하세요.

리프트 앤드 시프트

7 R을 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 인공 지능의 한 유형입니다. ML은 사물 인터넷(IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 기계 학습을 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 프로그램을 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 구축을 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 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 AWS에서 마이크로서비스 구현을 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 전략의 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 가이드와 마이그레이션 팩토리에 대한 설명을 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 가이드를 참조하세요. MRA는 AWS 마이그레이션 전략의 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 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 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.

OI

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 가이드를 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 가이드를 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 OAC도 참조하세요.

또는

운영 준비 상태 검토를 참조하십시오.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작되는 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 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 활성화를 참조하세요.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 상태 평가를 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 controls를 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 개념의 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 작업을 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 안내서를 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) 를 참조하십시오.

랜섬웨어

결제가 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 관리를 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.

리플랫포밍

7 R을 참조하십시오.

환매

7 R을 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 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 Implementing security controls on AWS의 Responsive controls를 참조하세요.

retain

7 R을 참조하십시오.

은퇴

7 R을 참조하십시오.

회전

공격자가 자격 증명에 액세스하는 것을 더 어렵게 만들기 위해 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

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 정보를 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 시크릿을 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 정책을 참조하세요.

서비스 엔드포인트

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

시엠

보안 정보 및 이벤트 관리 시스템을 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 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 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 Synthetics를 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 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 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 사용을 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.

웜

한 번 쓰고, 많이 읽으세요.

WQF

AWS 워크로드 검증 프레임워크를 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.