



에서 VMware Cloud의 ID 및 액세스 관리 AWS

AWS 권장 가이드



AWS 권장 가이드: 에서 VMware Cloud의 ID 및 액세스 관리 AWS

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

소개	1
수강 대상	2
목표 비즈니스 성과	2
ID 관리 개요	3
ID 페더레이션 및 SSO	4
일반 모범 사례	5
VMware ID 관리 서비스	7
VMware Cloud Services 콘솔	7
ID 및 액세스 관리	7
AWS 권장 사항	8
VMware vCenter Server	9
ID 및 액세스 관리	9
AWS 권장 사항	10
관련 VMware 서비스	12
의 VMware Cloud AWS	12
ID 및 액세스 관리	13
AWS 권장 사항	14
VMware NSX	14
ID 및 액세스 관리	15
AWS 권장 사항	16
VMware Aria Operations for Logs	16
ID 및 액세스 관리	17
AWS 권장 사항	17
VMware Aria Operations for Networks	18
ID 및 액세스 관리	18
AWS 권장 사항	19
VMware Aria Operations	19
ID 및 액세스 관리	19
AWS 권장 사항	20
VMware Live 사이버 복구	20
ID 및 액세스 관리	21
AWS 권장 사항	21
VMware HCX	22
ID 및 액세스 관리	22

AWS 권장 사항	23
VMware Live Site 복구	23
ID 및 액세스 관리	24
AWS 권장 사항	24
샘플 그룹 및 역할	25
다음 단계	29
리소스	30
관련 AWS 리소스	30
VMware 설명서	30
의 VMware Cloud AWS	30
VMware vCenter Server 및 vCenter Single Sign-On	30
VMware NSX	31
VMware HCX	31
VMware Aria 및 vRealize 제품군	31
VMware Live Site Recovery	31
VMware Live 사이버 복구	31
문서 기록	32
용어집	33
#	33
A	34
B	36
C	38
D	41
E	45
F	47
G	48
H	49
정보	51
L	53
M	54
O	58
P	60
Q	63
R	63
S	66
T	69

U	71
V	71
W	72
Z	73
.....	lxxiv

에서 VMware Cloud의 자격 증명 및 액세스 관리 AWS

Richard Milner-Watts, Abdenour Kansab 및 Chris Porter, Amazon Web Services

Vern Bolinius, VMware

2024년 9월([문서 기록](#))

알림

2024년 4월 30일부터의 VMware Cloud AWS 는 AWS 또는 채널 파트너가 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

ID 및 액세스 관리는 필요한 네트워크 리소스에만 액세스하도록 제한하는 것을 포함하여 승인된 사용자 및 애플리케이션에만 시스템 액세스를 제한하는 원칙입니다. 클라우드 환경에서 ID 및 액세스 관리 제어는 일반적으로 사용자, 사용자 그룹 및 애플리케이션을 식별, 인증 및 승인하는 데 사용하는 정책 및 서비스로 구성됩니다.

의 VMware Cloud는에서 VMware vSphere 기반 워크로드를 AWS 지원합니다 AWS 클라우드. 다양한 VMware 서비스와 도구를 사용하여 이 클라우드 인프라를 구성, 관리, 백업, 모니터링 및 분석할 수 있습니다. ID 및 액세스를 관리하는 데 사용하는 기능 및 제어는 서비스마다 다릅니다. 이 문서에서는 다음 VMware 서비스의 ID 및 액세스 관리 모범 사례와 권장 사항을 제공합니다.

- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks
- 의 VMware Cloud AWS
- VMware Cloud Services 콘솔
- VMware HCX
- VMware NSX
- VMware Live 사이버 복구
- VMware Live Site 복구
- VMware vCenter Server

이 가이드에서는 및 관련 VMware VMware 서비스의 VMware Cloud에 대한 자격 증명 및 액세스 관리의 개요 AWS 와 모범 사례를 제공합니다. 여기에는 각 서비스에 대한 간략한 설명과 해당 서비스에 대한 ID 액세스 및 관리 고려 사항이 설명되어 있습니다. 또한 VMware Cloud의 일부로 서비스를 구성하기 위한 권장 사항도 제공합니다 AWS.

Important

이 가이드에서 설명하는 많은 VMware 서비스는 다른 클라우드 또는 온프레미스 VMware 솔루션에서 사용됩니다. 이 가이드의 권장 사항과 모범 사례는 AWS의 VMware Cloud에만 해당됩니다. 다른 환경에는 이러한 권장 사항이 적용되지 않을 수 있습니다.

수강 대상

이 가이드는 클라우드 또는 하이브리드 환경에서 AWS 에서 VMware Cloud를 구현하는 일을 담당하는 아키텍트 및 보안 엔지니어를 위한 것입니다.

목표 비즈니스 성과

이 가이드는 다음을 수행하는 데 도움이 됩니다.

1. VMware Cloud on 및 관련 VMware VMware 서비스에 대한 다양한 자격 증명 AWS 및 액세스 관리 제어 이해
2. 에서 VMware Cloud를 안전하게 운영하는 데 도움이 되는 권장 모범 사례를 숙지합니다. AWS
3. 외부 ID 제공업체를 통한 페더레이션 인증에 사용할 수 있는 옵션 이해

ID 관리 개요

알림

2024년 4월 30일부터의 VMware Cloud AWS 는 AWS 또는 채널 파트너가 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

VMware는 다음과 같은 업계 표준 개념과 ID 계층 구조를 사용하여 식별, 인증 및 권한 부여를 관리합니다.

- 사용자는 일정 수준으로 환경에 액세스하는 개인입니다. 로컬 사용자를 생성하거나 페더레이션을 사용하여 외부 ID 제공업체로부터 사용자를 인증할 수 있습니다. 자세한 내용은 [ID 페더레이션 및 SSO 단원을 참조하십시오](#).
- 그룹은 사용자 모음을 논리적으로 그룹화하는 메커니즘을 제공합니다. 이렇게 하면 해당 사용자에게 일관된 권한을 부여하고 관리 오버헤드를 줄일 수 있습니다. 역할은 사용자 또는 그룹에 권한을 부여하는 데 사용됩니다. 자세한 내용은 [Roles and Permissions in the SDDC](#)(VMware 설명서)를 참조하세요.
- VMware Cloud의 조직은 하나 이상의 VMware 서비스에 대한 액세스를 제어합니다. 조직 내 서비스에 액세스하려면 사용자와 그룹이 조직에 속해 있어야 합니다. [ID 거버넌스 및 관리](#) 기능을 활성화하여 페더레이션형 ID가 VMware 조직에 대한 셀프 서비스 요청 멤버십을 허용하도록 할 수 있습니다. 자세한 내용은 [VMware Cloud Services 콘솔 단원을 참조하십시오](#).

권한은 특정 객체에 대한 액세스 권한을 부여하거나 상위 객체에서 상속될 수 있습니다. 사용자 또는 그룹에 중복되는 여러 권한이 할당되는 경우 가장 허용적인 권한이 적용됩니다. 자세한 내용은 [Hierarchical Inheritance of Permissions](#)(VMware 설명서)를 참조하세요.

이러한 구조적 요소를 사용하여 최소 권한 정책을 채택하고 사용자 요구 사항에 따라 인프라 내에 논리적 액세스 경계를 설정할 수 있습니다. 최소 권한은 작업을 수행하는 데 필요한 최소한의 액세스 권한만 사용자와 애플리케이션에 부여하는 원칙입니다. 무단 액세스가 발생하는 경우 이 업계 모범 사례는 공격자가 피해를 입히거나 민감한 데이터를 훔칠 수 있는 능력을 제한하는 데 도움이 될 수 있습니다. 또한 권한 있는 사용자의 경우에도 이 원칙을 통해 사용자가 보유해서는 안 되는 데이터에 액세스하는 것을 방지할 수 있습니다. 사용자에게 필요한 리소스에만 액세스할 수 있도록 하면 생산성이 향상되고 문제 해결 지원의 필요성도 줄어들 수 있습니다.

에서 VMware Cloud를 사용하는 경우 AWS자격 증명 및 액세스를 관리하기 위한 두 가지 기본 서비스 및 도구가 [VMware Cloud Services 콘솔](#) 있습니다 [VMware vCenter Server](#). 이 가이드의 후반부에서는 이러한 서비스에 대해 더 자세히 설명합니다.

ID 페더레이션 및 SSO

많은 회사에서 외부 ID 제공업체(idP)와 함께 페더레이션을 설정하려고 합니다. 이를 통해 사용자에게 AWS Single Sign-On(SSO) 환경을 제공할 수 있습니다. VMware Cloud와 vCenter Server는 모두 엔터프라이즈 페더레이션을 지원합니다.

- VMware Cloud는 SAML(Security Assertion Markup Language) 2.0 기반 IdP와 LDAP(Lightweight Directory Access Protocol)를 지원합니다. 자세한 내용은 [What is enterprise federation and how does it work with VMware Cloud Services](#)(VMware 설명서)를 참조하세요.
- 에서 VMware Cloud에서 vCenter Server를 운영하면 외부 IdP를 사용하여 vCenter Server에 AWS 페더레이션이 현재 지원되지 않습니다. LDAP를 통한 Microsoft Active Directory 사용을 지원하는 기본 제공 IdP만 사용할 수 있습니다. 자세한 내용은 [Identity Sources for vCenter Server with vCenter Single Sign-On](#)(VMware 설명서)을 참조하세요.

이 가이드에서 설명하는 기타 관련 VMware 서비스 중 일부는 IdP에서 직접 페더레이션도 지원합니다. 그러나 모든 서비스에서 페더레이션을 구성하면 사용자 관리 지점이 추가되어 관리하기 어려워집니다. 대신 VMware Cloud Services Console에서 그룹과 역할을 사용하여 공통 ID 소스를 사용하고 다른 VMware Cloud 서비스에 대한 권한을 구성할 수 있습니다. 또한 온프레미스 vCenter Server 인스턴스에서 동일한 ID를 사용하도록 Hybrid Linked Mode를 구성할 수 있습니다. 이렇게 하면 페더레이션 및 ID 관리 지점 수가 서비스 2개로 줄어듭니다. Hybrid Linked Mode에 대한 자세한 내용은 [Configuring Hybrid Linked Mode](#)(VMware 설명서)를 참조하세요.

일반 모범 사례

알림

2024년 4월 30일부터의 VMware Cloud AWS 는 AWS 또는 채널 파트너가 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

Important

이 가이드에서 설명하는 많은 VMware 서비스는 다른 클라우드 또는 온프레미스 VMware 솔루션에서 사용됩니다. 이 가이드의 권장 사항과 모범 사례는 AWS의 VMware Cloud에만 해당됩니다. 다른 환경에는 이러한 권장 사항이 적용되지 않을 수 있습니다.

VMware 클라우드 인프라에 대한 자격 증명 및 액세스를 관리하기 위해 다음 AWS 권장 사항을 고려하세요.

- 최소 권한 정책을 적용합니다. 역할 기반 액세스 제어(RBAC)로 사용자가 해당 기능을 수행하는 데 필요한 최소한의 권한과 액세스 권한을 부여합니다.
- 가능하면 개별 사용자가 아닌 그룹에 권한을 부여합니다.
- 로컬 사용자를 구성하지 않습니다. 외부 페더레이션형 ID 제공업체를 대상으로 사용자를 인증합니다.
- 모든 사용자에 대한 다중 인증을 구성합니다.
- 암호 정책에는 암호 강도 및 교체 요구 사항이 포함되어야 합니다.
- VMware 조직과 관련 서비스를 완벽하게 관리할 수 있는 응급 절차를 문서화합니다. 응급은 화재 경보기를 울릴 때 유리를 깨는 것에서 이름을 따온 것으로, 승인되고 감사된 프로세스를 사용하여 예외적인 상황에서 관리 권한을 신속하게 확보할 수 있는 수단을 말합니다.
- 온프레미스 데이터 센터 또는 여러 vCenter Server 인스턴스가 있는 경우 Hybrid Linked Mode를 사용하여 클라우드 vCenter Server 인스턴스를 온프레미스 vCenter Single Sign-On 도메인과 연결합니다. 이를 통해 단일 vSphere Client 인터페이스에서 클라우드 및 온프레미스 리소스를 관리할 수 있습니다.
- 가능하면 vCenter Server, HCX Cloud Manager 및 NSX Manager와 같은 관리 엔드포인트를 퍼블릭 인터넷이 아닌 내부 네트워크에서만 액세스할 수 있도록 구성합니다.

- 관리 목적으로 cloudadmin 계정과 같은 로컬 자격 증명을 사용하지 않습니다. 응급 절차에 사용할 수 있도록 이 계정을 예약합니다. 관리 로컬 사용자 계정을 사용하여 수행된 작업은 특정 개인에게 귀속될 수 없으므로 이러한 계정을 사용하여 책임 없이 변경할 수 있습니다.
- 루트 및 관리 사용자와 같은 로컬 계정의 암호를 강력한 값으로 변경하고 이러한 보안 인증을 감사된 암호 스토어에 안전하게 보관합니다. 이러한 암호에 대한 액세스 권한을 부여하기 위한 승인 프로세스를 수립합니다.
- VMware HCX를 사용하여 네트워크를 확장하는 경우와 같이 로컬 보안 인증이 장기간(예: 몇 개월 이상) 유지되는 경우 보안 인증을 교체하는 프로세스를 수립합니다.

이러한 권장 사항은의 VMware Cloud에 대한 모든 VMware 서비스 구성에 적용됩니다 AWS. 각 서비스에 대한 추가 권장 사항은 이 가이드의 뒷부분에서 다룹니다.

VMware ID 관리 서비스

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

에서 VMware Cloud를 사용하는 경우 AWS자격 증명 및 액세스를 관리하기 위한 두 가지 기본 서비스 및 도구가 [VMware Cloud Services 콘솔](#) 있습니다 [VMware vCenter Server](#).

VMware Cloud Services 콘솔

[VMware Cloud Services Console](#)(VMware 설명서)을 사용하면 VMware Cloud on을 포함하는 VMware Cloud 서비스 포트폴리오를 관리할 수 있습니다 AWS. 이 서비스에서는 다음을 수행할 수 있습니다.

- 사용자 및 그룹과 같은 엔터티 관리
- VMware Live Cyber Recovery 및 VMware Aria Suite와 같은 다른 클라우드 서비스에 대한 액세스를 제어하는 조직 관리
- 리소스 및 서비스에 역할 할당
- 조직에 액세스할 수 있는 OAuth 애플리케이션 보기
- 조직의 엔터프라이즈 페더레이션 구성
- 에서 VMware Aria 및 VMware Cloud와 같은 VMware Cloud 서비스 활성화 및 배포 AWS
- 청구 및 구독 관리
- VMware 지원 받기

ID 및 액세스 관리

VMware Cloud Services Console에서 사용자, 그룹, 역할 및 조직을 적절히 설정하면 최소 권한 액세스 정책을 구현할 수 있습니다.

VMware Cloud Services Console의 관리자는 VMware Cloud 환경 전체에서 권한을 변경하고 청구 정보와 같은 민감한 정보에 액세스할 수 있기 때문에 이 서비스에 대한 액세스를 보호하는 것은 매우 중

요합니다. 청구 및 지원과 같은 모든 콘솔 기능에 액세스하려면 사용자는 VMware Customer Connect 프로파일(구 MyVMware)과도 연결되어야 합니다.

VMware Cloud Services Console에서는 다음과 같은 유형의 역할을 사용하여 사용자 및 그룹에 권한을 부여합니다.

- 조직 역할 - 이러한 역할은 VMware Cloud 조직과 직접 관련이 있으며 VMware Cloud Services Console 내에서 권한을 부여합니다. 두 가지 표준 역할이 있습니다. 조직 소유자 역할에는 조직을 관리할 수 있는 전체 권한이 있습니다. 조직 멤버 역할에는 VMware Cloud Services Console에 대한 읽기 권한이 있습니다. 자세한 내용은 [What organization roles are available in VMware Cloud Services](#)(VMware 설명서)를 참조하세요.
- 서비스에 대한 역할 - 이 역할을 통해 특정 서비스를 사용할 권한을 할당할 수 있습니다. 예를 들어 DR Admin 서비스 역할이 있는 엔터티는 전용 서비스 콘솔에서 VMware Live Cyber Recovery를 관리할 수 있습니다. 조직 내에서 사용할 수 있는 모든 서비스에는 하나 이상의 관련 서비스 역할이 있습니다. 사용 가능한 서비스 역할에 대한 자세한 내용은 관심 있는 서비스에 대한 VMware 설명서를 참조하세요.

VMware Cloud Services Console은 인증 정책을 지원합니다. 이 정책은 사용자가 로그인할 때 다중 인증(MFA)이라고도 하는 두 번째 인증 토큰을 제공해야 한다고 규정할 수 있습니다.

이 서비스의 ID 및 액세스 관리에 대한 자세한 내용은 [Identity and Access Management](#)(VMware 설명서)를 참조하세요.

AWS 권장 사항

[일반 모범 사례](#) 외에도 AWS는 AWS의 VMware Cloud에 대해 VMware Cloud Services Console 구성 시 다음 사항을 권장합니다.

- 조직을 생성할 때 vmwarecloudroot@example.com과 같이 개인에게 속하지 않는 VMware Customer Connect 프로파일 및 연결된 회사 이메일 주소를 사용합니다. 이 계정은 서비스 또는 루트 계정으로 취급되어야 하며 사용자가 사용을 감사하고 이메일 계정에 대한 액세스를 제한해야 합니다. 사용자가 이 계정을 사용하지 않고도 조직에 액세스할 수 있도록 기업 ID 제공업체(idP)와 계정 페더레이션을 즉시 구성합니다. 페더레이션형 IdP 관련 문제를 해결하기 위한 응급 절차에 사용할 수 있도록 이 계정을 예약합니다.
- 조직의 페더레이션 자격 증명을 사용하여 VMware Live Cyber Recovery와 같은 다른 클라우드 서비스에 대한 액세스 권한을 부여합니다. 여러 서비스의 사용자 또는 페더레이션을 개별적으로 관리하지 마세요. 이렇게 하면 사용자가 회사에 입사하거나 퇴사하는 경우 등에 여러 서비스에 대한 액세스를 간편하게 관리할 수 있습니다.

- 조직 소유자 역할은 거의 할당하지 않습니다. 이 역할을 가진 엔터티는 조직의 모든 측면 및 관련 클라우드 서비스에 대한 전체 액세스 권한을 자신에게 부여할 수 있습니다.

VMware vCenter Server

[VMware vCenter Server](#)(VMware 웹 사이트)는 VMware vSphere 환경을 관리하기 위한 관리 영역입니다. vCenter Server에서는 가상 머신과 같은 vSphere 리소스에 액세스하고 VMware HCX 및 VMware Live Site Recovery와 같은 추가 기능에 액세스할 수 있는 엔터티를 관리합니다. vSphere 클라이언트 애플리케이션을 통해 vCenter Server를 관리합니다. vCenter Server에서는 다음을 수행할 수 있습니다.

- 가상 머신, VMware ESXi 호스트 및 VMware vSAN 스토리지를 관리합니다.
- vCenter Single Sign-On 구성 및 관리

온프레미스 데이터 센터가 있는 경우 Hybrid Linked Mode를 사용하여 클라우드 vCenter Server 인스턴스를 온프레미스 vCenter Single Sign-On 도메인에 연결할 수 있습니다. vCenter Single Sign-On 도메인에 Enhanced Linked Mode를 사용하여 연결된 여러 vCenter Server 인스턴스가 포함된 경우 해당 인스턴스가 클라우드 SDDC에 모두 연결됩니다. 이 모드를 사용하면 단일 vSphere Client 인터페이스에서 온프레미스 및 클라우드 데이터 센터를 보고 관리할 수 있으며, 온프레미스 데이터 센터와 클라우드 SDDC 간에 워크로드를 마이그레이션할 수 있습니다. 자세한 내용은 [Configuring Hybrid Linked Mode](#)(VMware 설명서)를 참조하세요.

ID 및 액세스 관리

VMware Cloud on용 [소프트웨어 정의 데이터 센터\(SDDCs\)](#)(VMware 웹 사이트)에서 vCenter Server를 운영하는 AWS방식은 온프레미스 SDDC와 유사합니다. 주된 차이점은의 VMware Cloud AWS 가 관리형 서비스라는 것입니다. 따라서 VMware는 호스트, 클러스터 및 관리 가상 머신 관리와 같은 특정 관리 작업을 담당합니다. 자세한 내용은 [What's Different in the Cloud?](#) 및 [Global permissions](#)(VMware 설명서)를 참조하세요.

VMware는 SDDC에 대한 일부 관리 작업을 수행하기 때문에 클라우드 관리자에게 필요한 권한은 온프레미스 데이터 센터의 관리자보다 적습니다. AWS SDDC에서 VMware Cloud를 생성하면 cloudadmin 사용자가 자동으로 생성되고 [CloudAdmin](#) 역할이 할당됩니다(VMware 설명서). 이 권한 있는 로컬 사용자 계정을 사용하여 vCenter Server와 vCenter Single Sign-On에 액세스할 수 있습니다. VMware Cloud VMware Services Console에 VMware Cloud on AWS Administrator 또는 관리자(제한 삭제) 서비스 역할이 있는 사용자는 cloudadmin 사용자의 자격 증명을 얻을 수 있습니다. CloudAdmin 역할에는 AWS SDDC의 VMware Cloud에 대해 vCenter Server에서 가능한 최대 권한이 있습니다. 이 서비

스 역할에 대한 자세한 내용은 [CloudAdmin Privileges](#)(VMware 설명서)를 참조하세요. cloudadmin 사용자는 AWS의 VMware Cloud의 vCenter Server에 사용할 수 있는 유일한 로컬 사용자입니다. 다른 사용자에게 액세스 권한을 부여하려면 외부 ID 소스를 사용합니다.

vCenter Single Sign-On은 보안 토큰 교환 인프라를 제공하는 인증 브로커입니다. 사용자가 vCenter Single Sign-On에 인증하면 해당 사용자는 API 호출을 사용하여 vCenter Server 및 기타 추가 서비스를 인증하는 데 사용할 수 있는 토큰을 받습니다. cloudadmin 사용자는 vCenter Server의 외부 ID 소스를 구성할 수 있습니다. 자세한 내용은 [Identity Sources for vCenter Server with vCenter Single Sign-On](#)(VMware 설명서)을 참조하세요.

vCenter Server에서는 다음과 같은 유형의 3가지 역할을 사용하여 사용자와 그룹에 권한을 부여합니다.

- 시스템 역할 - 이 역할은 편집하거나 삭제할 수 없습니다.
- 샘플 역할 - 이 역할은 자주 수행되는 작업의 조합을 나타냅니다. 이 역할을 복사, 편집 또는 삭제할 수 있습니다.
- 사용자 지정 역할 - 시스템 및 샘플 역할이 원하는 액세스 제어를 제공하지 않는 경우 vSphere Client에서 사용자 지정 역할을 생성할 수 있습니다. 기존 역할을 복제하고 수정하거나 새 역할을 생성할 수 있습니다. 자세한 내용은 [Create a vCenter Server Custom Role](#)(VMware 설명서)을 참조하세요.

SDDC 인벤토리의 각 객체에 대해 사용자 또는 그룹에 역할 하나만 할당할 수 있습니다. 단일 객체에 대해 사용자 또는 그룹에 기본 제공 역할 조합이 필요한 경우 2가지 옵션이 있습니다. 첫 번째 옵션은 필요한 권한이 있는 사용자 지정 역할을 생성하는 것입니다. 다른 옵션은 두 그룹을 생성하고 각 그룹에 기본 제공 역할을 할당한 다음 두 그룹에 사용자를 추가하는 것입니다.

AWS 권장 사항

[일반 모범 사례](#) 외에도 AWS는 AWS의 VMware Cloud에 대해 vCenter Server 구성 시 다음 사항을 권장합니다.

- cloudadmin 사용자 계정을 사용하여 vCenter Single Sign-On에서 외부 ID 소스를 구성합니다. 관리 목적으로 사용할 외부 ID 소스의 적절한 사용자를 할당한 다음 cloudadmin 사용자의 사용을 중단합니다. vCenter Single Sign-On 구성 시 모범 사례는 [Information Security and Access for vCenter Server](#)(VMware 설명서)를 참조하세요.
- vSphere Client에서 각 vCenter Server 인스턴스의 cloudadmin 자격 증명을 새 값으로 업데이트한 다음 안전하게 저장합니다. 이 변경 사항은 VMware Cloud Services Console에 반영되지 않습니다. 예를 들어, Cloud Services Console을 통해 보안 인증을 보면 원래 값이 표시됩니다.

Note

이 계정의 보안 인증을 분실한 경우 VMware 지원 팀에서 보안 인증을 재설정할 수 있습니다.

- 일상적인 액세스에 cloudadmin 계정을 사용하지 않습니다. 응급 절차의 일부로 사용할 수 있게 이 계정을 예약합니다.
- vCenter Server에 대한 네트워크 액세스를 프라이빗 네트워크로 제한합니다.

관련 VMware 서비스

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

이 장에서는 VMware Cloud와 관련된 다음 VMware 서비스에 대한 자격 증명 및 액세스를 관리하기 위한 모범 사례와 권장 사항을 제공합니다 AWS.

• VMware Cloud Services Console을 통해 관리되는 서비스:

- [의 VMware Cloud AWS](#)
- [VMware NSX](#)
- [VMware Aria Operations for Logs](#)
- [VMware Aria Operations for Networks](#)
- [VMware Aria Operations](#)
- [VMware Live 사이버 복구](#)

• VMware vCenter Server를 통해 관리되는 서비스:

- [VMware HCX](#)
- [VMware Live Site 복구](#)

이 가이드에서는 각 서비스에 대한 간략한 설명을 제공하고, 해당 서비스의 자격 증명 액세스 및 관리 제어에 대해 설명하고, VMware Cloud의 일부로 해당 서비스를 구성하기 위한 AWS 권장 사항을 포함합니다 AWS.

의 VMware Cloud AWS

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

[VMware Cloud on AWS](#) (VMware 설명서)는 온프레미스 VMware vSphere 기반 환경을 로 마이그레이션하고 확장하는 데 도움이 되도록 AWS 및 VMware에서 공동으로 설계된 서비스입니다 AWS 클라우드.

이 서비스에 대한 액세스 권한을 부여하는 조직에 속한 경우 VMware Cloud Services 콘솔을 AWS 통해서 VMware Cloud에 액세스할 수 있습니다. 의 VMware Cloud에서 다음을 AWS수행할 수 있습니다.

- SDDC를 생성하고 삭제합니다.
- SDDC 그룹을 관리합니다.
- 네트워킹 및 클러스터 파라미터를 포함한 SDDC를 관리합니다.
- VMware vCenter Server의 cloudadmin 사용자 보안 인증에 액세스합니다. 이 사용자에게 대한 자세한 내용은 이 가이드의 [VMware vCenter Server](#) 섹션을 참조하세요.
- VMware NSX의 cloud_admin 사용자 보안 인증에 액세스합니다. 이 사용자에게 대한 자세한 내용은 이 가이드의 [VMware NSX](#) 섹션을 참조하세요.
- VMware Live Site Recovery 및 VMware HCX와 같은 SDDCs 내에서 추가 기능 서비스를 활성화하고 배포합니다.
- HCX 및 VMware Live Site Recovery를 포함한 추가 기능 서비스를 위한 콘솔에 액세스합니다.

ID 및 액세스 관리

VMware Cloud Services 콘솔을 사용하여의 VMware Cloud에 대한 자격 증명 및 액세스를 관리합니다 AWS. 의 VMware Cloud의 경우 다음 AWS서비스 역할을 사용할 수 있습니다.

- 관리자 -이 역할은 VMware Cloud on에 대한 전체 액세스 권한을 가집니다 AWS.
- 관리자(Delete Restricted) AWS-이 역할은 SDDC 삭제 작업을 제외하고의 VMware Cloud에 대한 전체 액세스 권한을 갖습니다.
- NSX Cloud Admin
- NSX Cloud Auditor

Note

NSX Cloud Admin과 NSX Cloud Auditor는 VMware NSX 사용과 관련이 있습니다. 자세한 내용은 [VMware NSX](#) 단원을 참조하십시오.

Cloud Services Portal 내에서 SDDC에 액세스하려면 두 Administrator 역할 중 하나가 필요합니다. 두 NSX Cloud 역할 중 하나가 없는 사용자는 Cloud Services Portal 내의 SDDC 네트워킹 및 보안 탭에 액세스할 수 없으며 NSX 관리자 보안 인증에도 액세스할 수 없습니다.

AWS 권장 사항

[일반 모범 사례](#) 외에도 AWS 는 AWS의 VMware Cloud 구성 시 다음 사항을 권장합니다.

- 관리자에게 액세스 권한을 부여하려면 Administrator (Delete Restricted) 역할만 사용합니다. SDDC 를 삭제해야 하는 경우 응급 액세스를 위해 Administrator 역할을 예약합니다.
- 네트워킹 및 방화벽 구성에 액세스할 필요가 없는 사용자에게 NSX 역할을 부여하지 마세요. 자세한 내용은 이 안내서의 [VMware NSX](#) 섹션을 참조하세요.
- cloudadmin 로컬 사용자 계정의 암호를 강력한 값으로 변경하고 이러한 보안 인증을 감사된 암호 스토어에 안전하게 저장합니다. vSphere Web Client를 사용하여 VMware vCenter Server에서 이 암호를 변경할 수 있습니다.

VMware NSX

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

[VMware NSX](#)(VMware 설명서)는 스위칭, 라우팅, 방화벽 등의 기능을 갖춘 계층 2에서 계층 7까지 OSI(Open Systems Interconnection) 모델을 재현하는 네트워크 가상화 계층을 제공합니다. 두 가지 버전의 NSX가 있습니다. 원래 버전(NSX-V)을 사용하려면 vCenter Server도 배포해야 합니다. 최신 버전(NSX-T)은 vCenter Server와 분리되어 하이브리드 아키텍처를 지원할 수 있습니다. 의 VMware Cloud 는 NSX-T를 AWS 사용합니다.

NSX는 vSphere 및 vSAN과 함께 VMware Cloud on의 핵심 구성 요소입니다 AWS. NSX는 SDDC 내에서 모든 네트워킹 기능을 제공하고 오버레이 네트워킹과 네트워크 언더레이를 구성하는 AWS 기본 구성 요소 간의 상호 작용을 관리합니다. NSX는 리소스를 관리하기 위해 NSX API를 직접적으로 호출하는 vCenter Server, VMware HCX 등의 다른 서비스와 긴밀하게 연결되어 있습니다.

NSX에서는 다음을 수행할 수 있습니다.

- 스위칭 및 라우팅 관리
- VM 간 또는 네트워크와 퍼블릭 인터넷 간 인라인 검사를 위한 분산 방화벽 사용을 비롯한 방화벽 관리
- 가상 프라이빗 네트워크(VPN) 관리
- Dynamic Host Configuration Protocol(DHCP) 및 도메인 이름 시스템(DNS) 구성

VMware Cloud Services Console 또는 전용 NSX Manager 웹 사용자 인터페이스(UI)를 통해 NSX에 액세스할 수 있습니다. NSX Manager 웹 UI는 VMware Cloud Services Console에서 사용할 수 없는 몇 가지 추가 기능을 제공합니다. 자세한 내용은 [SDDC Network Administration with NSX Manager](#)(VMware 설명서)를 참조하세요.

AWS의 VMware Cloud에서 NSX에 액세스할 때 다음 사항을 참고하세요.

- VMware Cloud Services 콘솔을 통해 NSX에 액세스하려면 VMware Cloud on AWS Administrator 역할이 할당되어야 합니다. SDDC 네트워킹 및 보안 탭에서 NSX에 액세스할 수 있습니다. 이 역할에 대한 자세한 내용은 이 가이드의 [의 VMware Cloud AWS](#) 섹션을 참조하세요.
- SDDC 설정 탭에서 링크를 선택하거나 SDDC 요약 페이지에서 NSX Manager 열기를 선택하여 NSX Manager 웹 UI를 열 수 있습니다. 자세한 내용은 [Open NSX Manager](#)(VMware 설명서)를 참조하세요.
- SDDC가 PCI DSS(Payment Card Industry Data Security Standard) 모드인 경우 VMware Cloud Services Console의 네트워킹 및 보안 탭을 통해 NSX에 액세스할 수 없습니다. NSX Manager 웹 UI를 사용해야 합니다.

ID 및 액세스 관리

VMware Cloud Services Console을 사용하여 ID와 VMware NSX에 대한 액세스를 관리합니다. VMware Cloud on의 NSX의 경우 다음 AWS서비스 역할을 사용할 수 있습니다.

- NSX Cloud Admin – 이 역할은 AWS의 VMware Cloud로 VMware NSX 기능을 관리할 수 있습니다.
- NSX Cloud Auditor – 이 역할은 NSX 서비스 설정 및 이벤트를 볼 수 있지만 변경할 수는 없습니다.

Note

이름은 다르지만 이러한 역할은 VMware NSX Cloud 서비스와는 관련이 없습니다.

NSX에 액세스할 수 있는 사용자는 다음과 같습니다.

- cloud_admin 로컬 사용자 - 기본 제공되고 권한이 높은 로컬 NSX 사용자입니다. NSX Cloud Admin 역할이 있는 사용자는 이 사용자 계정의 자격 증명에 액세스할 수 있습니다. 이름은 비슷하지만 cloud_admin 사용자는 cloudadmin@vmc.local vCenter Single Sign-On 로컬 사용자와 다릅니다.
- VMware Cloud Services Console에서 NSX Cloud Admin 서비스 역할 또는 NSX Cloud Auditor 서비스 역할을 할당받은 사용자입니다. 이러한 사용자는 VMware Cloud Services Console 사용자이거나 외부 페더레이션 사용자일 수 있습니다.
- LDAP를 통해 ID 소스에서 NSX에 대한 액세스 권한을 직접 부여받은 사용자입니다.

AWS 권장 사항

[일반 모범 사례](#) 외에도 AWS 는 AWS의 VMware Cloud에 대해 NSX 구성 시 다음 사항을 권장합니다.

- 회사에 네트워킹 및 방화벽 관리를 담당하지만 SDDC 관리는 담당하지 않는 사용자가 있는 경우 해당 사용자에게 NSX 역할 중 하나를 부여하되 Administrator 역할은 부여하지 마세요. 이러한 사용자는 NSX Manager 웹 UI를 통해 NSX에 액세스해야 합니다.
- cloud_admin 로컬 사용자 계정의 암호를 강력한 값으로 변경하고 이러한 보안 인증을 감사된 암호 스토어에 안전하게 저장합니다. 이 암호를 변경하려면 VMware 지원 팀에 문의해야 합니다.
- NSX 내에서 외부 사용자에게 직접 액세스 권한을 부여하지 마세요. 대신 VMware Cloud Services Console에서 엔터프라이즈 페더레이션을 설정한 다음 역할과 그룹을 사용하여 이 서비스에 대한 액세스 권한을 부여합니다.

VMware Aria Operations for Logs

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

[VMware Aria Operations for Logs](#)(구 VMware vRealize Log Insight Cloud)(VMware 설명서)는 VMware SDDC에서 생성된 로그 데이터를 시각화하고 쿼리하는 데 도움이 되는 로그 스토리지 및 분석 도구입니다. VMware Aria Operations for Logs에서는 다음을 수행할 수 있습니다.

- vRealize Operations의 온프레미스 인스턴스와 통합
- 모든 유형의 시스템 생성 로그 데이터 수집 및 분석
- 알림 구성
- 다른 VMware 서비스의 로그 모니터링 및 분석

이 중앙 집중식 로그 관리 서비스에는 두 가지 버전이 있습니다. VMware vRealize Log Insight는 SDDC 내에서 어플라이언스로 실행할 수 있는 온프레미스 버전입니다. VMware Aria Operations for Logs는 서비스형 소프트웨어(SaaS) 버전입니다. 의 VMware Cloud는 클라우드 버전을 기본 로깅 서비스로 AWS 사용하므로 변경할 수 없습니다. 온프레미스 버전을 사용하는 경우 클라우드 인스턴스에서 온프레미스 인스턴스로 로그를 전달해야 합니다.

VMware Aria Operations for Logs는 VMware Cloud on에 포함되어 있습니다 AWS. 포함된 버전은 수집 용량과 스토리지 보존 기간이 제한되어 있습니다. 필요한 경우 프리미엄 구독으로 업그레이드하여 이러한 제한을 늘릴 수 있습니다. 자세한 내용은 [Subscriptions and Billing](#)(VMware 설명서)을 참조하세요.

ID 및 액세스 관리

VMware Cloud Services Console을 사용하여 ID와 VMware Aria Operations for Logs에 대한 액세스를 관리합니다. VMware Aria Operations for Logs는 VMware Cloud Services Console에서 구성된 페더레이션형 ID 및 그룹을 포함하여 동일한 사용자를 사용합니다. 이 서비스에 대한 권한을 부여하려면 VMware Aria Operations for Logs 내에서 서비스 역할을 할당하거나 사용자 지정 역할을 구성합니다. 자세한 내용은 [Service Roles](#)(VMware 설명서)를 참조하세요.

VMware vRealize Log Insight에는 두 가지 기본 역할이 있습니다. Administrator 역할에는 전체 액세스 및 제어 권한이 있으며, User 역할에는 읽기 권한이 있고 대시보드를 생성할 수 있습니다. 사용자 지정 역할을 사용하여 특정 데이터 세트에만 액세스 권한을 부여할 수 있습니다. 이러한 데이터 세트에는 사용자가 사용할 수 있는 로그 데이터를 제한하는 필터가 포함되어 있습니다. 자세한 내용은 [Create a Data Set](#)(VMware 설명서)를 참조하세요.

AWS 권장 사항

이 가이드의 앞부분에 설명한 [일반 모범 사례](#)를 따르세요. 이 서비스의 ID 및 액세스 관리에 대한 추가 권장 사항은 없습니다.

VMware Aria Operations for Networks

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

VMware Aria Operations for Networks(구 VMware vRealize Network Insight Cloud)는 vRealize Network Insight의 SaaS 버전입니다. [VMware vRealize Network Insight](#)(VMware 설명서)는 워크로드의 트래픽 흐름을 이해하는 데 도움이 됩니다. 이 서비스를 사용하여 네트워킹 문제를 진단하고 워크로드 세분화를 지원하는 방화벽 규칙을 모델링할 수 있습니다. VMware Aria Operations for Networks에서는 다음을 수행할 수 있습니다.

- 하이브리드 및 멀티 클라우드 환경 보기
- 트래픽 흐름 문제 해결 및 분석
- 애플리케이션 검색 및 분석
- 워크로드 간 종속성 매핑

이 서비스에는 세 가지 버전이 있습니다. VMware vRealize Network Insight는 온프레미스 전용 버전입니다. VMware Aria Operations for Networks는 SaaS 버전입니다. vRealize Network Insight Universal은 온프레미스 솔루션 또는 페더레이션형 클라우드 SaaS 솔루션으로 배포될 수 있습니다. 모든 버전은의 VMware Cloud와 호환됩니다 AWS.

ID 및 액세스 관리

VMware Cloud Services Console을 사용하여 ID와 VMware Aria Operations for Networks에 대한 액세스를 관리합니다. VMware Aria Operations for Networks는 VMware Cloud Services Console에서 구성된 페더레이션형 ID 및 그룹을 포함하여 동일한 사용자를 사용합니다. VMware Aria Operations for Networks의 경우 다음과 같은 서비스 역할을 사용할 수 있습니다.

- Administrator – 이 역할에는 전체 액세스 및 제어 권한이 있습니다.
- Member – 이 역할에는 제한된 액세스 권한이 있습니다.
- Auditor – 이 역할에는 읽기 전용 권한이 있습니다.

AWS 권장 사항

이 가이드의 앞부분에 설명한 [일반 모범 사례](#)를 따르세요. 이 서비스의 ID 및 액세스 관리에 대한 추가 권장 사항은 없습니다.

VMware Aria Operations

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

[VMware Aria Operations](#)(구 VMware vRealize Operations Cloud)(VMware 설명서)는 AWS의 VMware Cloud를 위한 운영 관리 플랫폼입니다. 이 서비스는 인공지능 및 기계 학습(AI/ML)을 사용하여 하이브리드 클라우드 배포에서 애플리케이션과 인프라를 최적화, 계획 및 확장하는 데 도움을 줍니다. VMware Aria Operations에서는 다음을 수행할 수 있습니다.

- 성능 및 용량에 대한 AI/ML 기반 최적화 권장 사항 보기
- 규정 준수 및 리소스 구성 관리
- 고객 문제 해결 또는 알림 대응과 같은 문제를 해결하는 데 도움이 되는 도구에 액세스
- [관리 팩](#)(VMware 설명서)을 사용하여 이 서비스의 모니터링, 문제 해결 및 수정 기능 확장

이 운영 관리 서비스에는 두 가지 버전이 있습니다. VMware vRealize Operations는 SDDC 내에서 어플라이언스로 실행할 수 있는 온프레미스 버전입니다. VMware Aria Operations는 vRealize Operations의 서비스형 소프트웨어(SaaS) 버전입니다. 두 버전 모두 VMware Cloud on과 호환됩니다. AWS. 의 VMware Cloud AWS 는 관리형 서비스이며 일부 리소스에 대한 액세스가 제한되므로 일부 vRealize Operations 기능이 지원되지 않습니다. 자세한 내용은 [Known Limitations](#)(VMware 설명서)를 참조하세요.

ID 및 액세스 관리

VMware Cloud Services Console을 사용하여 ID와 VMware Aria Operations에 대한 액세스를 관리합니다. VMware Aria Operations는 VMware Cloud Services Console에서 구성하는 페더레이션형 ID를 포함하여 동일한 사용자를 사용합니다. 이 서비스에 대한 권한을 부여하려면 VMware Aria Operations

내에서 서비스 역할을 할당하거나 사용자 지정 역할을 구성합니다. 사용 가능한 서비스 역할에 대한 자세한 내용은 [Roles and Privileges](#)(VMware 설명서)를 참조하세요.

기본 제공 역할에는 Administrator, GeneralUser, ReadOnly의 세 가지가 있으며, 필요한 경우 특정 권한 요구 사항에 맞게 사용자 지정 역할을 만들 수 있습니다. 그룹을 생성하여 여러 사용자의 권한을 관리하는 데 따른 관리 오버헤드를 최소화할 수 있습니다.

VMware vRealize Operations의 온프레미스 버전은 로컬 사용자를 지원하며 클라우드 버전과 온프레미스 버전 모두 페더레이션 사용자를 지원합니다. 그러나 외부 ID 제공업체에 대한 사용자 페더레이션은 vRealize Operations의 온프레미스 버전과 클라우드 버전에 따라 다릅니다. 온프레미스 버전의 경우 LDAP를 통해 외부 IdP의 사용자를 직접 페더레이션하거나 vCenter Server에서 페더레이션한 ID를 사용할 수 있습니다. 클라우드 버전의 경우 페더레이션 사용자를 포함하여 VMware Cloud Services Console에서 구성한 것과 동일한 사용자를 사용합니다.

AWS 권장 사항

[일반 모범 사례](#) 외에도 AWS는 AWS의 VMware Cloud에 대해 VMware Aria Operations 구성 시 다음 사항을 권장합니다.

- 사용자를 직접 페더레이션하지 않습니다. 클라우드 버전의 경우 VMware Cloud Services Console에서 사용자를 페더레이션한 다음 역할과 그룹을 사용하여 이 서비스에 대한 액세스 권한을 부여합니다. 이 서비스의 온프레미스 버전에서는 인증된 소스의 ID를 사용하거나 AWS Single Sign-On(SSO)을 활성화합니다. 자세한 내용은 [Authentication sources](#) 및 [Configure a Single Sign-On Source](#)(VMware 설명서)를 참조하세요.

VMware Live 사이버 복구

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

[VMware Live Cyber Recovery](#)(VMware 설명서)는 재해 복구에 대한 계층화된 접근 방식을 제공하는 서비스형 재해 복구(DRaaS) 솔루션입니다. Recovery Point Objective(RPO)와 Recovery Time Objective(RTO)에 대한 비용과 기간을 조정하여 해당 워크로드의 요구 사항을 충족할 수 있습니다. 이

를 통해 안정적인 보호와 효율적인 재해 복구 리소스 사용 사이에서 균형을 맞출 수 있습니다. VMware Live Cyber Recovery에서 다음을 수행할 수 있습니다.

- 가상 머신 백업 생성
- 내구성이 뛰어난 클라우드 스토리지에 백업 저장
- 온디맨드부터 상시 대기 모드까지 복원 대상을 위한 유연한 배포 옵션 중에서 선택
- 사용자 지정 RPO 및 RTO 구성

ID 및 액세스 관리

VMware Cloud Services 콘솔을 사용하여 VMware Live Cyber Recovery에 대한 자격 증명 및 액세스를 관리합니다. VMware Live Cyber Recovery는 연합 자격 증명 및 VMware Cloud Services 콘솔에서 구성된 그룹을 포함하여 동일한 사용자를 사용합니다. 이 서비스에 대한 권한을 부여하려면 VMware Live Cyber Recovery 서비스 역할을 할당하거나 VMware Live Cyber Recovery 내에서 사용자 지정 역할을 생성할 수 있습니다. 사용 가능한 서비스 역할에 대한 자세한 내용은 [VMware Live Cyber Recovery 최종 사용자 역할](#)(VMware 설명서)을 참조하세요.

VMware Live Cyber Recovery에는 서비스 운영에 사용할 수 있는 몇 가지 기본 제공 역할이 포함되어 있습니다.

- Administrator – API 토큰에 대한 액세스를 제외한 전체 제어 권한이 있습니다.
- Auditor – 사용자 관리를 제외한 사용자 인터페이스에 대한 읽기 전용 액세스 권한이 있습니다. 규정 준수 보고서에 액세스할 수 있습니다.
- DR Admin – 재해 복구 계획을 생성, 테스트 및 실행합니다.
- Backup Admin – 보호 사이트와 보호 그룹을 관리합니다. VM을 복원할 수 있는 액세스 권한이 있습니다.
- Plan Tester – 재해 복구 계획을 세우고 테스트 복구를 실행합니다.
- SDDC Admin – SDDC를 관리합니다.

AWS 권장 사항

이 가이드의 앞부분에 설명한 [일반 모범 사례](#)를 따르세요. 이 서비스의 ID 및 액세스 관리에 대한 추가 권장 사항은 없습니다.

VMware HCX

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

[VMware HCX](#)(VMware 설명서)는 SDDC 간 워크로드 마이그레이션을 지원하는 애플리케이션 이동성 플랫폼입니다. VMware HCX는의 VMware Cloud에 포함되어 AWS 있으며 워크로드를 마이그레이션 하는 데 사용할 수 있습니다. VMware HCX에서는 다음을 수행할 수 있습니다.

- SDDC 간 멀티 사이트 메시 구성
- HCX 사이트 간 네트워크 확장
- 가상 머신 마이그레이션

ID 및 액세스 관리

VMware vCenter Server를 사용하여 ID와 VMware HCX에 대한 액세스를 관리합니다. VMware HCX를 사용하려면 vCenter Server 및 NSX에 대한 액세스를 포함하여 리소스 및 마이그레이션을 생성하고 관리하기 위해 다른 VMware 서비스에 액세스할 수 있어야 합니다. VMware HCX에는 다음과 같은 두 가지 구성 요소 서비스가 있습니다.

- HCX Cloud Manager – VMware Cloud Services Console에서 VMware HCX for the SDDC를 활성화 합니다. 그러면 선택한 SDDC 내에 HCX Cloud Manager 어플라이언스가 설치됩니다. 자세한 내용은 [Deploying the HCX Installer OVA in the vSphere Client](#)(VMware 설명서)를 참조하세요. 배포 후에는 vCenter Server cloudadmin 보안 인증을 사용하여 HCX Cloud Manager 서비스에 액세스할 수 있습니다.
- HCX Connector – HCX Cloud Manager 서비스를 통해 HCX Connector Open Virtualization Archive(OVA) 파일을 받을 수 있습니다. 이 파일을 사용하여 모든 vCenter Server 인스턴스에 HCX Cloud Manager 어플라이언스를 설치하고 해당 인스턴스를 VMware HCX의 마이그레이션 소스로 설정합니다. 각 HCX Connector 인스턴스에는 고유한 관리자 및 루트 보안 인증이 있습니다.

두 구성 요소 서비스를 모두 배포한 후에는 vCenter Server를 통해 VMware HCX에 액세스할 수 있습니다. Administrators vCenter Single Sign-On 그룹에는 자동으로 HCX Administrator 역할이 부여됩니다.

다. HCX를 설치하면 vCenter Single Sign-On에 많은 추가 역할과 권한이 추가됩니다. 이를 사용하여 다양한 사용자 유형에 따라 VMware HCX에 대한 세분화된 액세스 제어를 생성합니다.

AWS 권장 사항

[일반 모범 사례](#) 외에도 AWS 는 AWS의 VMware Cloud에 대해 VMware HCX 구성 시 다음 사항을 권장합니다.

- 게이트웨이 방화벽 규칙을 사용하여 HCX Cloud Manager 서비스에 대한 네트워크 액세스를 제한할 수 있습니다.
- 온프레미스 HCX Connector admin 및 root user 보안 인증을 안전하게 저장합니다. 회사 정책에 따라 이러한 보안 인증 교체를 고려하세요. VMware는 HCX Cloud Manager를 위해 사용자를 대신하여 이러한 보안 인증을 관리합니다.
- 온프레미스 HCX Connector 인스턴스의 경우 다양한 HCX 사용자 유형의 요구 사항에 맞는 사용자 지정 HCX 역할을 생성하는 것을 고려해 보세요. 예를 들어, HCX를 설정하고 관리하는 사용자에게는 더 허용적인 역할을 만들고 마이그레이션만 관리하는 사용자에게는 덜 허용적인 역할을 생성합니다.
- VMware HCX를 VMware Cloud on과 페어링 AWS할 때는 cloudadmin 사용자를 사용해야 합니다.
- HCX Cloud를 VMware Cloud on과 페어링할 때 AWS SDDC의 VMware Cloud와 Active Directory 간에 AWS인증이 지원되지 않습니다. 자세한 내용은 [\[VMC on AWS\] AD unsupported for HCX Cloud to Cloud setup](#)(VMware Knowledge Base 문서 90433)을 참조하세요.

VMware Live Site 복구

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

[VMware Live Site Recovery](#)(VMware 설명서)는 온프레미스 환경을 위한 VMware Site Recovery Manager 서비스를 기반으로 하는 온디맨드 DRaaS(서비스형 재해 복구) 솔루션입니다. VMware Live Site Recovery에서 다음을 수행할 수 있습니다.

- 복제, 오케스트레이션 및 자동화를 구현하여 사이트 장애 발생 시 워크로드를 보호할 수 있습니다.

- SDDC 보호를 지원하는 엔드 투 엔드 재해 복구 솔루션 생성

ID 및 액세스 관리

VMware vCenter Server를 사용하여 VMware VMware Live Site Recovery에 대한 자격 증명 및 액세스를 관리합니다. VMware Live Site Recovery는 사용자를 대신하여 가상 머신 복제 또는 전원 끄기와 같은 작업을 수행합니다. VMware Live Site Recovery는 역할과 권한을 사용하여 올바른 권한이 있는 사용자만 복구 계획의 모든 단계를 실행하는 등 복구 작업을 수행할 수 있도록 합니다.

자세한 내용은 [VMware Live Site Recovery Privileges, Roles, and Permissions\(VMware 설명서\)](#)를 참조하십시오. VMware

페더레이션형 ID를 사용하여 vCenter Server에 액세스하는 경우 Hybrid Linked Mode를 사용하여 이러한 그룹에 엔터티를 추가해야 합니다. 자세한 내용은 [Configuring Hybrid Linked Mode\(VMware 설명서\)](#)를 참조하십시오.

AWS 권장 사항

외에도는 VMware VMware Cloud용 VMware Live Site Recovery를 구성할 때 다음을 [일반 모범 사례](#) AWS 권장합니다 AWS.

- 소스 사이트와 대상 사이트 모두에서 사용자에게 동일한 역할을 할당해야 합니다. 그러면 보호된 객체와 복구된 객체가 동일한 권한을 갖게 됩니다.
- 하이브리드 연결 모드를 사용하여 vCenter Server 내의 페더레이션 자격 증명에 대한 역할 할당을 관리합니다.
- VMware Live Site Recovery는 SDDC 내에서만 프라이빗 IP 주소를 사용합니다. [일반 모범 사례](#)에 따라 AWS의 VMware Cloud vCenter가 프라이빗 IP 주소로 확인되는지 확인합니다.

샘플 그룹 및 역할

알림

2024년 4월 30일부터의 VMware Cloud AWS 는 AWS 또는 채널 파트너가 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

다음 표에는 AWS의 VMware Cloud를 사용하기 위한 ID 및 액세스 관리 전략의 예가 나와 있습니다. 여기에는 사용자 페르소나, 페르소나가 액세스해야 하는 VMware 서비스, 조직 및 그룹 멤버, 할당된 역할, 사용된 ID 유형(예: 로컬 사용자 또는 페더레이션형 ID)이 요약되어 있습니다. 이 표를 시작점으로 삼아 이 가이드에서 권장하는 모범 사례를 준수하는 회사 전략을 설계하세요.

사용자 페르소나	액세스한 서비스	VMware Cloud 샘플 그룹 이름	VMware Cloud 서비스 역할	vCenter Single Sign-On 샘플 그룹 이름	vCenter Single Sign-On 역할	보안 인증 원본
조직 응급	VMware Cloud Services 콘솔	없음	조직 소유자	없음	없음	로컬 사용자(서비스 계정 이메일 주소)
VMware 관리자	VMware Cloud Services 콘솔 vCenter Server HCX	vmware_admins	조직 소유자	vmware_admins	관리자	페더레이션형 ID 제공업체

사용자 페르소나	액세스한 서비스	VMware Cloud 샘플 그룹 이름	VMware Cloud 서비스 역할	vCenter Single Sign-On 샘플 그룹 이름	vCenter Single Sign-On 역할	보안 인증 원본
	VMware Live Site 복구 VMware Live 사이버 복구 vRealize Operations					
백업 관리자	vCenter Server	없음	없음	vmware_backup	파워 유저	페더레이션형 ID 제공업체
재해 복구 관리자	vCenter Server VMware Cloud Services 콘솔 VMware Live Site 복구 VMware Live 사이버 복구	vmware_dr	조직 멤버 DR Admin DR SDDC Admin	vmware_dr	SrmAdministrator HmsCloudAdmin	페더레이션형 ID 제공업체

사용자 페르소나	액세스한 서비스	VMware Cloud 샘플 그룹 이름	VMware Cloud 서비스 역할	vCenter Single Sign-On 샘플 그룹 이름	vCenter Single Sign-On 역할	보안 인증 원본
VMware 운영자	VMware Cloud Services 콘솔 vCenter Server HCX vRealize Operations	vmware_ops	조직 멤버 vROps Administrator	vmware_ops	파워 유저	페더레이션형 ID 제공업체
네트워킹 팀	VMware Cloud Services 콘솔 vCenter Server	vmware_networks	조직 멤버 NSX Cloud Admin	vmware_networks	읽기 전용	페더레이션형 ID 제공업체

사용자 페르소나	액세스한 서비스	VMware Cloud 샘플 그룹 이름	VMware Cloud 서비스 역할	vCenter Single Sign-On 샘플 그룹 이름	vCenter Single Sign-On 역할	보안 인증 원본
보안 팀	VMware Cloud Services 콘솔 vCenter Server HCX(임시 액세스) VMware Live Site 복구 VMware Live 사이버 복구 vRealize Operations	vmware_security	조직 멤버 vROps ReadOnly	vmware_security	읽기 전용	페더레이션형 ID 제공업체
감사	VMware Cloud Services 콘솔 vCenter Server	vmware_audit	조직 멤버	vmware_audit	읽기 전용	페더레이션형 ID 제공업체

다음 단계

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

이 가이드에서는 AWS 및 관련 VMware VMware 서비스에서 VMware Cloud의 자격 증명 및 액세스를 관리하는 데 권장되는 모범 사례를 다루었습니다. 이러한 권장 사항은 클라우드 및 하이브리드 클라우드 인프라를 보호하고 무단 액세스를 방지하는 데 도움이 되도록 설계되었지만 확장 가능하고 효율적이도록 설계되었습니다. 사용자를 그룹에 배정한 다음 그룹에 역할을 할당하면 권한을 더 빠르게 부여 또는 제한하고 사용자를 개별적으로 구성하는 데 따르는 오버헤드를 최소화할 수 있습니다. 또한 외부 ID 제공업체 및 vCenter Single Sign-On과의 페더레이션을 사용하여 사용자에게 원활한 싱글 사인온 환경을 제공할 수 있습니다.

[샘플 그룹 및 역할](#) 표를 사용하여 회사에 적합한 ID 및 액세스 관리 전략 설계를 시작하세요. 이 가이드의 권장 사항을 검토한 후 [리소스](#) 섹션에 제공된 링크를 검토하는 것이 좋습니다. 이러한 리소스를 통해 VMware Cloud 서비스와 이 가이드에 설명된 모범 사례를 구성하는 방법에 대해 자세히 알아볼 수 있습니다.

리소스

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

관련 AWS 리소스

- [VMware Cloud on AWS 개요 및 운영 모델](#)
- [의 VMware Cloud에서 워크로드에 대한 재해 복구 옵션 AWS](#)
- [에서 VMware Cloud에 대한 스토리지 오프로드 옵션 구성 AWS](#)
- [에서 VMware Cloud를 AWS 사용하여에 VMware SDDC 배포 AWS](#)
- [VMware HCX를 AWS 사용하여에서 VMware SDDC를 VMware Cloud로 마이그레이션](#)

VMware 설명서

의 VMware Cloud AWS

- [클라우드 서비스를 위한 엔터프라이즈 페더레이션 설정](#)
- [VMware Cloud Services Identity and Access Management](#)

VMware vCenter Server 및 vCenter Single Sign-On

- [vSphere의 권한 부여 이해](#)
- [의 VMware Cloud에서 vSphere 관리 AWS](#)
- [vCenter Single Sign-On으로 vSphere 인증](#)
- [vCenter Single Sign-On ID 소스 구성](#)
- [권한의 계층적 상속](#)
- [vCenter Server의 정보 보안 및 액세스](#)
- [일반 작업에 필요한 vSphere 권한](#)

VMware NSX

- [NSX Administration Guide](#)
- [NSX-T Data Center에 대한 정보 보안 및 액세스](#)

VMware HCX

- [VMware HCX Documentation](#)
- [VMware HCX 사용자 계정 및 역할 요구 사항](#)

VMware Aria 및 vRealize 제품군

- [VMware vRealize 운영 설명서](#)
- [vRealize Operations 클라우드의 역할 및 권한](#)
- [VMware vRealize Log Insight 데이터시트](#)
- [로그에 대한 VMware Aria 작업 시작하기](#)
- [VMware Cloud Services 설명서](#)
- [vRealize Network Insight 사용자 관리](#)

VMware Live Site Recovery

- [VMware Live Site Recovery 설명서](#)
- [VMware Live Site Recovery 권한, 역할 및 권한](#)

VMware Live 사이버 복구

- [VMware Live 사이버 복구 설명서](#)
- [VMware Live 사이버 복구 최종 사용자 역할](#)

문서 기록

알림

2024년 4월 30일부터 AWS 또는 채널 파트너가의 VMware Cloud AWS 를 더 이상 재판매하지 않습니다. 서비스는 Broadcom을 통해 계속 사용할 수 있습니다. 자세한 내용은 AWS 담당자에게 문의하는 것이 좋습니다.

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

변경 사항	설명	날짜
VMware 서비스 제품	VMware Cloud Disaster Recovery를 VMware Live Cyber Recovery로 대체하고 VMware Site Recovery를 VMware Live Site Recovery로 대체했습니다. 자세한 내용은 VMware Live Recovery 릴리스 정보 를 참조하세요.	2024년 9월 4일
VMware HCX 액세스	VMware Cloud용 VMware HCX를 구성하기 위한 AWS 권장 사항을 업데이트했습니다 AWS.	2023년 6월 5일
최초 게시	—	2022년 11월 3일

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 버전으로 마이그레이션합니다.
- 리플랫폼(리프트 앤드 리세이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예:에서 온프레미스 Oracle 데이터베이스를 Oracle용 Amazon Relational Database Service(RDS)로 마이그레이션합니다 AWS 클라우드.
- 재구매(드롭 앤드 쇼프) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예:의 EC2 인스턴스에서 온프레미스 Oracle 데이터베이스를 Oracle로 마이그레이션합니다 AWS 클라우드.
- 재배포(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 나중에 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

A

ABAC

[속성 기반 액세스 제어를](#) 참조하세요.

추상화된 서비스

[관리형 서비스를](#) 참조하세요.

ACID

[원자성, 일관성, 격리, 내구성](#)을 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 마이그레이션](#)보다 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 예로는 SUM 및 MAX가 있습니다.

AI

[인공 지능](#)을 참조하세요.

AIOps

[인공 지능 작업을](#) 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 사용할 수 있는 보안 접근 방식입니다.

애플리케이션 포트폴리오

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

인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 [What is Artificial Intelligence?](#)를 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 가이드](#)를 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 AWS](#)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 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 되는 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 웹 사이트](#)와 [AWS CAF 백서](#)를 참조하십시오.

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

잘못된 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 [봇](#)입니다.

BCP

[비즈니스 연속성 계획](#)을 참조하세요.

동작 그래프

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

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. [Endianness](#)도 참조하세요.

바이너리 분류

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

블룸 필터

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

블루/그린(Blue/Green) 배포

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

bot

인터넷을 통해 자동화된 작업을 실행하고 인적 활동 또는 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같은 일부 봇은 유용하거나 유용합니다. 잘못된 봇이라고 하는 일부 다른 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 것입니다.

봇넷

[맬웨어](#)에 감염되고 [봇](#) 셰이더 또는 봇 운영자라고 하는 단일 당사자에 의해 제어되는 봇 네트워크입니다. Botnet은 봇과 봇의 영향을 확장하는 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.

브레이크 글래스 액세스

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는데 액세스할 수 있는 빠른 방법입니다. 자세한 내용은 Well-Architected 지침의 [브레이크 글래스 포로시저 구현 표시기](#)를 AWS 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 클라우드 채택 프레임워크](#)를 참조하세요.

canary 배포

최종 사용자에게 버전의 느린 증분 릴리스입니다. 확신이 드는 경우 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

[Cloud Center of Excellence](#)를 참조하세요.

CDC

[변경 데이터 캡처](#)를 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 장애 또는 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 전달](#)을 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 게시물](#)을 참조하세요.

클라우드 컴퓨팅

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

클라우드 운영 모델

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

클라우드 채택 단계

조직이 로 마이그레이션할 때 일반적으로 거치는 4단계: AWS 클라우드

- 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 가이드](#)를 참조하세요.

CMDB

[구성 관리 데이터베이스](#)를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리에는 GitHub 또는가 포함됩니다Bitbucket Cloud. 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 예상 상태에서 변경됩니다. 이로 인해 워크로드가 규정 미준수 상태가 될 수 있으며 일반적으로 점진적이고 의도하지 않습니다.

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 적합성 팩을 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 [적합성 팩](#)을 참조하세요.

지속적 통합 및 지속적 전달(CI/CD)

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

CV

[컴퓨터 비전](#)을 참조하세요.

D

저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리 전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected Framework에서 보안 원칙의 구성 요소입니다. 자세한 내용은 [데이터 분류](#)를 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 분산된 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 일반적으로 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

[데이터베이스 정의 언어](#)를 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 컨트롤을 AWS 추가하여 리소스를 보호할 수 있습니다. 예를 들어, 심층 방어 접근 방식은 다단계 인증, 네트워크 세분화 및 암호화를 결합할 수 있습니다.

위임된 관리자

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

[환경](#)을 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 Implementing security controls on AWS의 [Detective controls](#)를 참조하십시오.

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 스키마](#)에서 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블입니다. 차원 테이블 속성은 일반적으로 텍스트 필드 또는 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 일반적으로 쿼리 제약, 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)

[재해](#)로 인한 가동 중지 시간과 데이터 손실을 최소화하는 데 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 [Disaster Recovery of Workloads on AWS: Recovery in the Cloud](#)를 참조하세요.

DML

[데이터베이스 조작 언어](#)를 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 방법](#)을 참조하십시오.

DR

[재해 복구](#)를 참조하세요.

드리프트 감지

기존 구성과의 편차 추적. 예를 들어 AWS CloudFormation 를 사용하여 [시스템 리소스의 드리프트를 감지](#)하거나 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 [랜딩 존의 변경 사항을 감지](#)할 수 있습니다.

DVSM

[개발 값 스트림 매핑](#)을 참조하세요.

E

EDA

[탐색 데이터 분석](#)을 참조하세요.

EDI

[전자 데이터 교환](#)을 참조하세요.

엣지 컴퓨팅

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

전자 데이터 교환(EDI)

조직 간의 비즈니스 문서 자동 교환. 자세한 내용은 [전자 데이터 교환이란 무엇입니까?](#)를 참조하세요.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 사이버텍스트로 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 엔드포인트](#)를 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 생성](#)을 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 암호화](#)를 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 마 이그레이션 전략의 에픽에 대한 자세한 내용은 [프로그램 구현 가이드](#)를 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 스키마](#)의 중앙 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블에는 측정값이 포함된 열과 차원 테이블에 대한 외래 키가 포함된 열의 두 가지 유형이 포함됩니다.

빠른 실패

개발 수명 주기를 줄이기 위해 자주 증분 테스트를 사용하는 철학입니다. 애자일 접근 방식의 중요한 부분입니다.

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 그래디언트와 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.

몇 장의 샷 프롬프트

유사한 작업을 수행하도록 요청하기 전에 작업과 원하는 출력을 보여주는 몇 가지 예제를 [LLM](#)에 제공합니다. 이 기법은 컨텍스트 내 학습을 적용하여 모델이 프롬프트에 포함된 예제(샷)에서 학습합니다. 퓨샷 프롬프트는 특정 형식 지정, 추론 또는 도메인 지식이 필요한 작업에 효과적일 수 있습니다. [제로샷 프롬프트도 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 캡처](#)를 통해 연속 데이터 복제를 사용하여 최대한 짧은 시간 내에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

[파운데이션 모델을 참조하세요.](#)

파운데이션 모델(FM)

일반화 및 레이블 지정되지 않은 데이터의 대규모 데이터 세트에 대해 훈련된 대규모 딥 러닝 신경망입니다. FMs은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 작업을 수행할 수 있습니다. 자세한 내용은 [파운데이션 모델이란 무엇입니까?](#)를 참조하세요.

G

생성형 AI

대량의 데이터에 대해 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트 및 오디오와 같은 새 콘텐츠 및 아티팩트를 생성할 수 있는 [AI](#) 모델의 하위 집합입니다. 자세한 내용은 [생성형 AI란 무엇입니까?](#)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 제한](#)을 참조하십시오.

Gitflow 워크플로

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

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조업에서는 골든 이미지를 사용하여 여러 디바이스에 소프트웨어를 프로비저닝할 수 있으며 디바이스 제조 작업의 속도, 확장성 및 생산성을 개선하는 데 도움이 됩니다.

브라운필드 전략

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

가드레일

조직 단위(OU) 전체에서 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 중요 규칙입니다. 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책과 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, 이는 AWS Config Amazon GuardDuty AWS Security Hub, , 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 데이터 세트에서 보류된 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교하여 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 리플랫폼 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

핫 데이터

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

핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 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.

정보

laC

[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 참조하십시오.](#)

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 적용 또는 수정하는 대신 프로덕션 워크로드를 위한 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 [변경 가능한 인프라](#)보다 본질적으로 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 [변경 불가능한 인프라를 사용한 배포](#) 모범 사례를 참조하세요.

인바운드(수신) VPC

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

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 참조하기 위해 2016년에 [Klaus Schwab](#)에서 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 구축](#)을 참조하십시오.

검사 VPC

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

사물 인터넷(IoT)

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

IT 정보 라이브러리(TIL)

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

IT 서비스 관리(TSM)

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

ITIL

[IT 정보 라이브러리](#)를 참조하세요.

ITSM

[IT 서비스 관리](#)를 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 설정](#)을 참조하십시오.

대규모 언어 모델(LLM)

방대한 양의 데이터를 기반으로 사전 훈련된 딥 러닝 [AI](#) 모델입니다. LLM은 질문 답변, 문서 요약, 텍스트를 다른 언어로 변환, 문장 완성과 같은 여러 작업을 수행할 수 있습니다. 자세한 내용은 [LLMs](#) 참조하십시오.

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 적용](#)을 참조하십시오.

리프트 앤드 시프트

[7R](#)을 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. [Endianness](#)도 참조하세요.

LLM

[대규모 언어 모델을](#) 참조하세요.

하위 환경

[환경을](#) 참조하세요.

M

기계 학습(ML)

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

기본 브랜치

[브랜치를](#) 참조하세요.

맬웨어

컴퓨터 보안 또는 개인 정보 보호를 손상하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 중단하거나, 민감한 정보를 유출하거나, 무단 액세스를 가져올 수 있습니다. 맬웨어의 예로는 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하며 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB는 관리형 서비스의 예입니다. 이를 추상화된 서비스라고도 합니다.

제조 실행 시스템(MES)

원재료를 작업 현장의 완성된 제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

[마이그레이션 가속화 프로그램을](#) 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 결과를 검사하여 조정하는 전체 프로세스입니다. 메커니즘은 작동 시 자체를 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 [메커니즘 구축](#)을 참조하세요.

멤버 계정

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

MES

[제조 실행 시스템을](#) 참조하세요.

메시지 대기열 원격 측정 전송(MQTT)

리소스가 제한된 [IoT](#) 디바이스에 대한 [게시/구독](#) 패턴을 기반으로 하는 경량 M2M(machine-to-machine) 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 마이크로 서비스를 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 전략](#)의 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 가이드](#)와 [마이그레이션 팩토리에 대한 설명](#)을 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)

로 마이그레이션하기 위한 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다 AWS 클라우드. 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 가이드](#)를 참조하십시오. MRA는 [AWS 마이그레이션 전략](#)의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 로 마이그레이션하는 데 사용되는 접근 방식입니다 AWS 클라우드. 자세한 내용은 이 용어집의 [7R 항목을 참조하고 대규모 마이그레이션을 가속화하기 위해 조직 동원을 참조하세요.](#)

ML

[기계 학습](#)을 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 [의 애플리케이션 현대화 전략을 참조하세요 AWS 클라우드.](#)

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 [의 애플리케이션에 대한 현대화 준비 상태 평가를 참조하세요 AWS 클라우드.](#)

모놀리식 애플리케이션(모놀리식 유형)

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

MPA

[마이그레이션 포트폴리오 평가를 참조하세요.](#)

MQTT

[메시지 대기열 원격 측정 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 워크로드를 위해 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework는 [변경 불가능한 인프라](#)를 모범 사례로 사용할 것을 권장합니다.

O

OAC

[오리진 액세스 제어를](#) 참조하세요.

OAI

[오리진 액세스 ID](#)를 참조하세요.

OCM

[조직 변경 관리](#)를 참조하세요.

오프라인 마이그레이션

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

OI

[작업 통합](#)을 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](#)를 참조하세요.

Open Process Communications - 통합 아키텍처(OPC-UA)

산업 자동화를 위한 M2M(Machinemachine-to-machine) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계와 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 가능한 장애의 범위를 이해, 평가, 예방 또는 줄이는 데 도움이 되는 질문 체크리스트 및 관련 모범 사례입니다. 자세한 내용은 AWS Well-Architected Framework의 [운영 준비 검토\(ORR\)](#)를 참조하세요.

운영 기술(OT)

물리적 환경과 함께 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조에서 OT 및 정보 기술(IT) 시스템의 통합은 [Industry 4.0](#) 혁신의 핵심 초점입니다.

운영 통합(OI)

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

조직 트레일

조직의 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는 AWS 계정에서 생성된 추적입니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서의 [Creating a trail for an organization](#)을 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 가이드](#)를 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 [OAC](#)도 참조하십시오.

ORR

[운영 준비 상태 검토](#)를 참조하세요.

OT

[운영 기술을](#) 참조하세요.

아웃바운드(송신) VPC

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

P

권한 경계

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

PLM

[제품 수명 주기 관리](#)를 참조하세요.

정책

권한을 정의하거나(자격 [증명 기반 정책](#) 참조), 액세스 조건을 지정하거나([리소스 기반 정책](#) 참조), 조직의 모든 계정에 대한 최대 권한을 정의할 수 있는 객체 AWS Organizations 입니다([서비스 제어 정책](#) 참조).

다국어 지속성

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

포트폴리오 평가

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

조건자

false 일반적으로 WHERE 절에 있는 true 또는를 반환하는 쿼리 조건입니다.

조건자 푸시다운

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

예방적 제어

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

보안 주체

작업을 수행하고 리소스에 액세스할 수 있는 AWS 있는의 엔티티입니다. 이 엔티티는 일반적으로 , AWS 계정 IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 [역할 용어 및 개념](#)의 보안 주체를 참조하십시오.

설계에 따른 개인 정보 보호

전체 개발 프로세스를 통해 개인 정보를 고려하는 시스템 엔지니어링 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](#).

사전 예방적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 [보안 제어](#)입니다. 이러한 제어는 리소스가 프로비저닝되기 전에 리소스를 스캔합니다. 리소스가 컨트롤을 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 [제어 참조 가이드](#)를 참조하고 보안 [제어 구현의 사전](#) 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도, 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리.

프로덕션 환경

[환경](#)을 참조하세요.

프로그래밍 가능한 로직 컨트롤러(PLC)

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

프롬프트 체인

한 [LLM](#) 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 작업을 하위 작업으로 나누거나 예비 응답을 반복적으로 구체화하거나 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)

마이크로서비스 간의 비동기 통신을 지원하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 [MES](#)에서 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 지침과 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

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

RAG

[Retrieval Augmented Generation](#)을 참조하세요.

랜섬웨어

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

RASCI 매트릭스

[책임, 책임, 상담, 정보 제공\(RACI\)을 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.

재설계

[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 리전은 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 [계정에서 사용할 수 있는 지정을 참조 AWS 리전 하세요.](#)

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.](#)

release

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

[7R을 참조하세요.](#)

리플랫폼

[7R을 참조하세요.](#)

재구매

[7R을 참조하세요.](#)

복원력

중단에 저항하거나 복구할 수 있는 애플리케이션의 기능입니다. 에서 복원력을 계획할 때 [고가용성](#) 및 [재해 복구](#)가 일반적인 고려 사항입니다 AWS 클라우드. 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 조연자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원자를 포함하면 매트릭스를 RASCI 매트릭스라고 하고, 지원자를 제외하면 RACI 매트릭스라고 합니다.

대응 제어

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

retain

[7R을 참조하세요.](#)

사용 중지

[7R을 참조하세요.](#)

검색 증강 세대(RAG)

응답을 생성하기 전에 [LLM](#)이 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 의미 검색을 수행할 수 있습니다. 자세한 내용은 [RAG란 무엇입니까?](#)를 참조하십시오.

교체

공격자가 보안 인증 정보에 액세스하는 것을 더 어렵게 만들기 위해 [보안 암호](#)를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

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

RPO

[복구 시점 목표를](#) 참조하세요.

RTO

[복구 시간 목표를](#) 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 조직 내 모든 사용자에게 대해 IAM에서 사용자를 생성하지 않고도 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 [SAML 2.0 기반 페더레이션 정보](#)를 참조하십시오.

SCADA

[감독 제어 및 데이터 획득](#)을 참조하세요.

SCP

[서비스 제어 정책](#)을 참조하세요.

secret

에는 암호 또는 사용자 자격 증명과 같이 암호화된 형식으로 저장하는 AWS Secrets Manager 기밀 또는 제한된 정보가 있습니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 [Secrets Manager 설명서의 Secrets Manager 보안 암호에 무엇이 있습니까?](#)를 참조하세요.

설계별 보안

전체 개발 프로세스를 통해 보안을 고려하는 시스템 엔지니어링 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가이드라인입니다. 보안 제어에는 [예방](#), [탐지](#), [대응](#) 및 [사전](#) 예방의 네 가지 주요 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 응답 자동화

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

서버 측 암호화

데이터를 AWS 서비스 수신하는가 대상에서 데이터를 암호화합니다.

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 엔드포인트](#)를 참조하십시오.

서비스 수준에 관한 계약(SLA)

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

서비스 수준 표시기(SLI)

오류율, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정입니다.

서비스 수준 목표(SLO)

서비스 [수준 지표](#)로 측정되는 서비스의 상태를 나타내는 대상 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 모델](#)을 참조하십시오.

SIEM

[보안 정보 및 이벤트 관리 시스템을](#) 참조하세요.

단일 장애 지점(SPOF)

애플리케이션의 중요한 단일 구성 요소에 장애가 발생하여 시스템이 중단될 수 있습니다.

SLA

[서비스 수준 계약을](#) 참조하세요.

SLI

[서비스 수준 표시기를](#) 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 [에서 애플리케이션 현대화에 대한 단계별 접근 방식을 참조하세요 AWS 클라우드](#).

SPOF

[단일 장애 지점을](#) 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 [데이터 웨어하우스](#) 또는 비즈니스 인텔리전스용으로 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 압도

하고 대체하는 것과 비슷합니다. [Martin Fowler](#)가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 [컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET\(ASMX\) 웹 서비스를 점진적으로 현대화하는 방법](#)을 참조하십시오.

서브넷

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

감독 제어 및 데이터 획득(SCADA)

제조에서 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 시스템을 테스트합니다. [Amazon CloudWatch Synthetics](#)를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

[LLM](#)에 컨텍스트, 지침 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 및 필터링할 수 있습니다. 자세한 내용은 [AWS 리소스에 태그 지정](#)을 참조하십시오.

대상 변수

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

작업 목록

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

테스트 환경

[환경을](#) 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.

전송 게이트웨이

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 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

[환경](#)을 참조하세요.

V

정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수행하는 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 그룹에 대해 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대 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.

WORM

[쓰기를 한 번, 많이 읽기를 참조하세요.](#)

WQF

[AWS 워크로드 검증 프레임워크](#)를 참조하세요.

한 번 쓰기, 많이 읽기(WORM)

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

Z

제로데이 익스플로잇

[제로데이 취약성](#)을 활용하는 공격, 일반적으로 맬웨어입니다.

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 프롬프트

[LLM](#)에 작업을 수행하기 위한 지침을 제공하지만 작업에 도움이 될 수 있는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 작업을 처리해야 합니다. 제로샷 프롬프트의 효과는 작업의 복잡성과 프롬프트의 품질에 따라 달라집니다. [스크린샷이 거의 없는 프롬프트도 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.