AWS 백서

SageMaker 스튜디오 관리 모범 사례

SageMaker 스튜디오 관리 모범 사례: AWS 백서

Table of Contents

SageMaker Studio 관리 모범 사례

게시 날짜: 2023년 4월 25일 (문서 수정)

요약

Amazon SageMaker Studio는 모든 기계 학습(ML) 개발 단계를 수행할 수 있는 단일한 웹 기반 시각적 인터페이스를 제공하여 데이터 과학 팀 생산성을 향상시킵니다. SageMaker Studio는 모델을 구축, 훈련 및 평가하는 데 필요한 각 단계에 대하여 완전한 액세스, 제어 및 가시성을 제공합니다.

이 백서에서는 운영 모델, 도메인 관리, 자격 증명 관리, 권한 관리, 네트워크 관리, 로깅, 모니터링 및 사용자 지정을 포함한 여러 주제의 모범 사례를 설명합니다. 여기서 설명하는 모범 사례는 다중 테넌트 배포를 포함한 엔터프라이즈 SageMaker Studio 배포를 위한 것입니다. 이 문서는 ML 플랫폼 관리자, ML 엔지니어 및 ML 아키텍트를 대상으로 합니다.

귀사는 Well-Architected입니까?

AWS Well-Architected Framework는 클라우드에서 시스템을 구축할 때 귀사에서 내리는 결정의 장단점을 이해하는 데 도움이 됩니다. 프레임워크의 6가지 요소를 사용하면 신뢰성 있고, 안전하며, 효율적이고, 비용 효율적이며, 지속 가능한 시스템을 설계하고 운영하기 위한 아키텍처 모범 사례를 살펴볼 수 있습니다. AWS Management Console에서 무료로 제공되는 AWS Well-Architected Tool을 사용하면 각 요소에 대한 일련의 질문에 답하는 방법으로, 모범 사례와 비교하여 워크로드를 검토할 수 있습니다.

Machine Learning Lens에서는, AWS 클라우드에서 기계 학습 워크로드를 설계, 배포 및 구축하는 방법에 중점을 둡니다. 이 Lens는 Well-Architected Framework에 설명된 모범 사례에 추가됩니다.

소개

SageMaker Studio를 ML 플랫폼으로서 관리하는 경우, 워크로드 증가에 따라 ML 플랫폼을 확장하는 데 도움이 되도록 정보에 입각한 결정을 내릴 때 참고할 모범 사례 지침이 필요합니다. ML 플랫폼을 프로비저닝, 운영 및 확장하려면 다음 사항을 고려하세요.

- 적합한 운영 모델을 선택하고 비즈니스 목표에 맞게 ML 환경을 구성하세요.
- 사용자 ID에 대한 SageMaker Studio 도메인 인증을 어떻게 설정할지 선택하고 도메인 수준 제한을 고려하세요.

- 세분화된 액세스 제어 및 감사를 위해 사용자의 ID 및 인증을 ML 플랫폼에 페더레이션하는 방법을 결정하세요.
- ML 페르소나의 다양한 역할에 대한 권한 및 가드레일을 설정하는 것을 고려해 보세요.
- ML 워크로드의 민감도, 사용자 수, 인스턴스 유형, 앱, 시작된 작업을 고려하여 Virtual Private Cloud(VPC) 네트워크 토폴로지를 계획하세요.
- 암호화를 통해 저장 데이터와 전송 중 데이터를 분류하고 보호하세요.
- 규정 준수를 위해 다양한 애플리케이션 프로그래밍 인터페이스(API)와 사용자 활동을 기록하고 모니터링하는 방법을 고려해 보세요.
- 자체 이미지와 수명 주기 구성 스크립트를 사용하여 SageMaker Studio 노트북 환경을 사용자 지정하세요.

운영 모델

운영 모델은 조직이 확장 가능하고 일관되며 효율적인 방식으로 비즈니스 가치를 제공하도록 지원하기 위해 사람, 프로세스 및 기술을 통합하는 프레임워크입니다. ML 운영 모델은 조직 전체의 팀을 위한 표준 제품 개발 프로세스를 제공합니다. 규모, 복잡성, 비즈니스 동인에 따라 운영 모델을 구현하기 위한 세 가지 모델이 있습니다.

- 중앙 집중식 데이터 과학 팀 — 이 모델에서는 모든 데이터 과학 활동이 단일 팀 또는 조직 내에서 중앙 집중화됩니다. 이는 모든 사업부가 이 팀에 데이터 과학 프로젝트를 맡기는 COE(Center of Excellence) 모델과 유사합니다.
- 분산된 데이터 과학 팀 — 이 모델에서는 데이터 과학 활동이 다양한 비즈니스 기능 또는 부서 또는 다양한 제품군에 따라 분산됩니다.
- 페더레이션된 데이터 과학 팀 — 이 모델에서는 코드 리포지토리, 지속적 통합 및 지속적 전달(CI/CD) 파이프라인 등과 같은 공유 서비스 기능은 중앙 집중식 팀에 의해 관리되며 각 사업부 또는 제품 수준 기능은 분산된 팀에 의해 관리됩니다. 이는 각 사업부에 자체 데이터 과학 팀이 있는 허브 앤 스포크 모델과 비슷하지만 이러한 사업부 팀은 중앙 집중식 팀과 활동을 조정합니다.

프로덕션 사용 사례를 위해 첫 번째 스튜디오 도메인을 출시하기로 결정하기 전에 운영 모델과 환경 구성을 위한 AWS 모범 사례를 고려해 보세요. 자세한 내용은 다중 계정을 사용한 AWS 환경 구성을 참조하세요.

다음 섹션에서는 각 운영 모델의 계정 구조를 구성하는 방법에 대한 지침을 제공합니다.

권장 계정 구조

이 섹션에서는 조직의 운영 요구 사항에 따라 시작하고 수정할 수 있는 운영 모델 계정 구조를 간략하게 소개합니다. 어떤 운영 모델을 선택하든 다음과 같은 일반적인 모범 사례를 구현하는 것이 좋습니다.

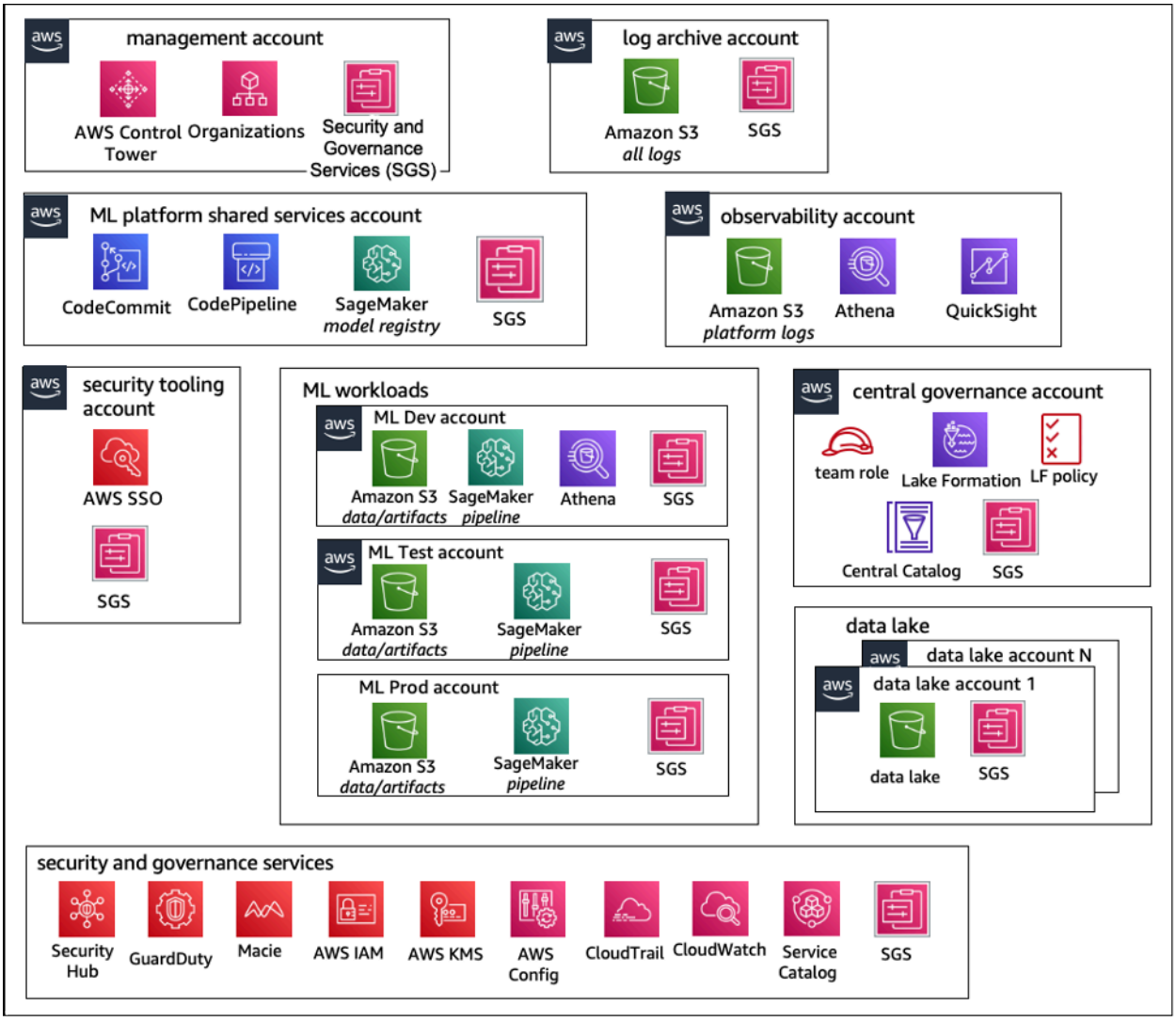
- 계정의 설정, 관리, 거버넌스에 AWS Control Tower를 사용하세요.
- ID 제공업체(idP)와 AWS IAM Identity Center를 통해 ID를 중앙 집중화하고 위임된 관리자 보안 도구 계정을 사용하여 워크로드에 안전하게 액세스할 수 있도록 하세요.
- 개발, 테스트 및 프로덕션 워크로드에 걸쳐 계정 수준 격리를 통해 ML 워크로드를 실행합니다.
- ML 워크로드 로그를 로그 아카이브 계정으로 스트리밍한 다음, 관찰성 계정에서 로그 분석을 필터링하고 적용합니다.
- 데이터 액세스를 프로비저닝, 제어 및 감사하기 위한 중앙 집중식 거버넌스 계정을 운영하세요.

- 적절한 예방 및 탐지 가드레일이 포함된 보안 및 거버넌스 서비스(SGS)를 각 계정에 내장하여 조직 및 워크로드 요구 사항에 따라 보안 및 규정 준수를 보장하십시오.

중앙 집중식 모델 계정 구조

이 모델에서 ML 플랫폼 팀은 다음을 제공할 책임이 있습니다.

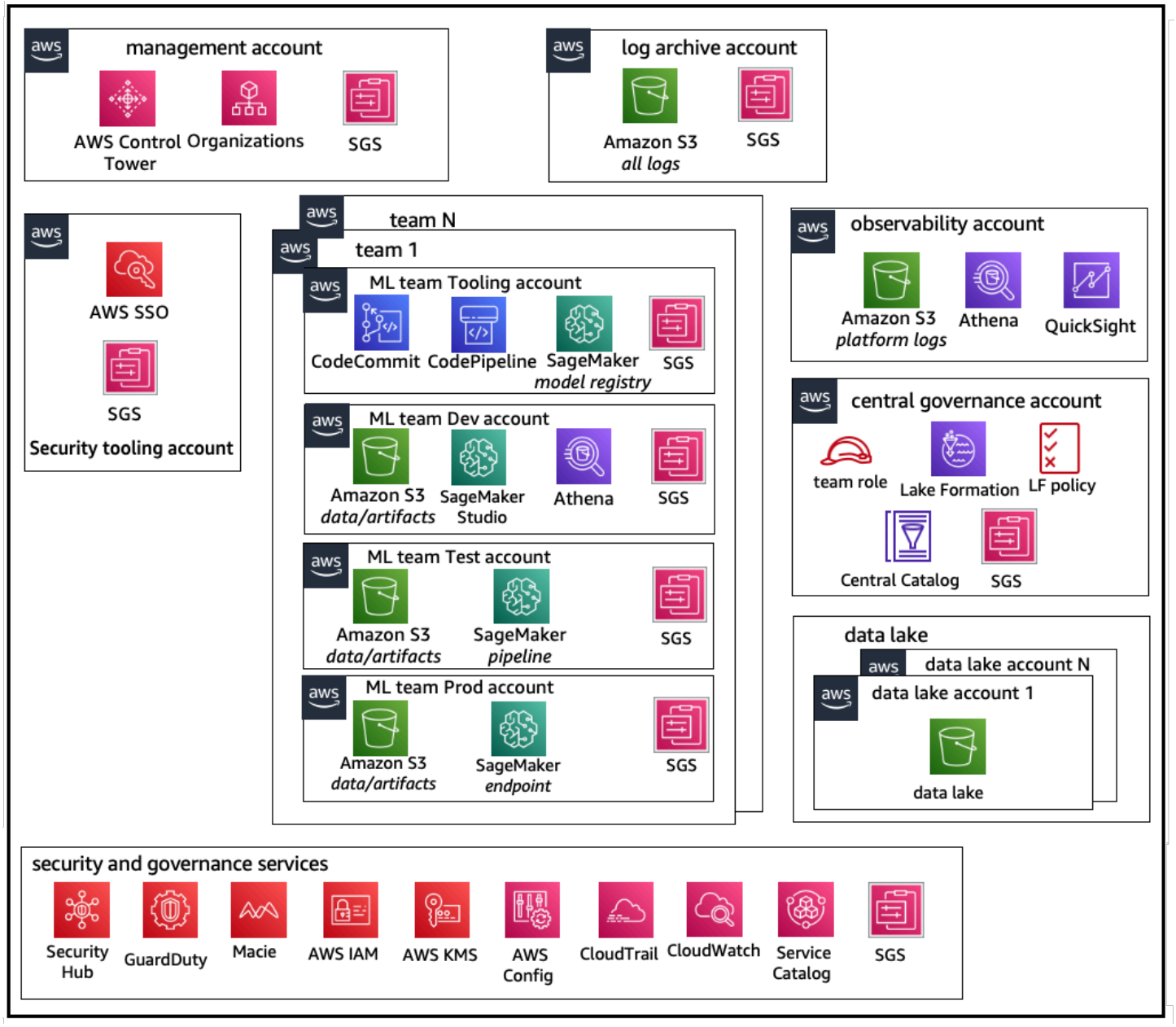
- 데이터 과학 팀 전체의 기계 학습 및 운영(MLOps) 요구 사항을 해결하는 공유 서비스 도구 계정.
- 데이터 과학 팀 간에 공유된 ML 워크로드 개발, 테스트 및 프로덕션 계정
- 각 데이터 과학 팀 워크로드가 분리되어 실행되도록 하는 거버넌스 정책.
- 일반적인 모범 사례.



중앙 집중식 운영 모델 계정 구조

분산된 모델 계정 구조

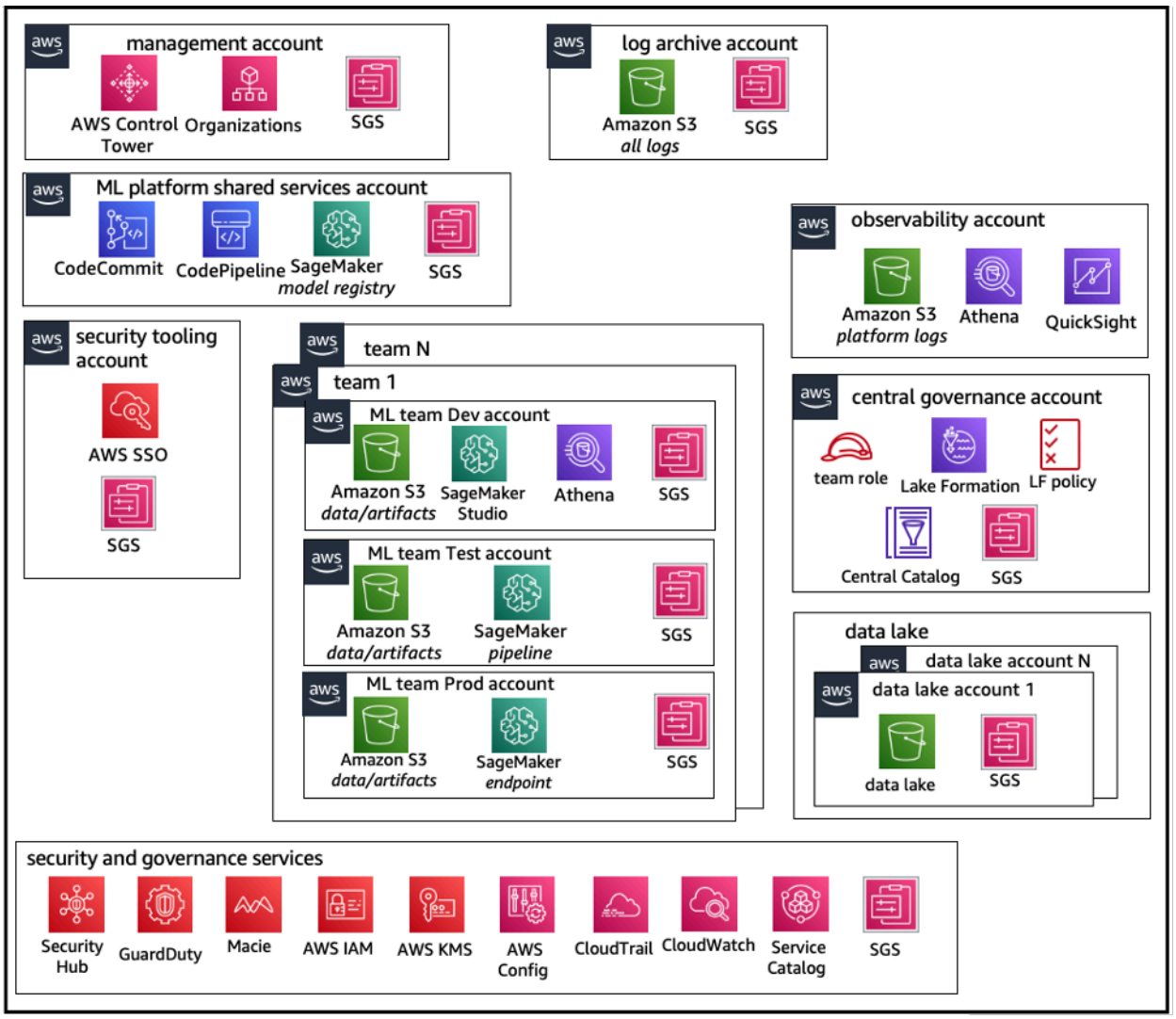
이 모델에서는 각 ML 팀이 ML 계정 및 리소스의 프로비저닝, 관리, 거버넌스를 위해 독립적으로 운영됩니다. 하지만 ML 팀은 중앙 집중식 관찰성 및 데이터 거버넌스 모델 접근 방식을 사용하여 데이터 거버넌스 및 감사 관리를 단순화하는 것이 좋습니다.



분산된 운영 모델 계정 구조

페더레이션된 모델 계정 구조

이 모델은 중앙 집중식 모델과 비슷하지만 주요 차이점은 각 데이터 과학/ML 팀이 자체 개발/테스트/프로덕션 워크로드 계정 세트를 보유하여 ML 리소스를 강력하게 물리적으로 격리하고 각 팀이 다른 팀에 영향을 주지 않고 독립적으로 확장할 수 있다는 것입니다.



페더레이션된 운영 모델 계정 구조

ML 플랫폼 멀티테넌시

멀티테넌시는 단일 소프트웨어 인스턴스가 여러 개의 개별 사용자 그룹을 지원할 수 있는 소프트웨어 아키텍처입니다. 테넌트는 소프트웨어 인스턴스에 대한 특정 권한으로 공통 액세스를 공유하는 사용자 그룹입니다. 예를 들어 여러 ML 제품을 구축하는 경우 액세스 요구 사항이 비슷한 각 제품 팀을 테넌트 또는 팀으로 간주할 수 있습니다.

SageMaker Studio 인스턴스(예: SageMaker 도메인) 내에서 여러 팀을 구현할 수 있지만, 여러 팀을 단일 ageMaker Studio 도메인으로 통합할 때는 블래스트 반경, 비용 귀속, 계정 수준 제한과 같은 장단점을 비교해 보세요. 다음 섹션에서 이러한 장단점 및 모범 사례에 대해 자세히 알아보십시오.

절대적인 리소스 격리가 필요한 경우 서로 다른 계정의 각 테넌트에 대해 SageMaker Studio 도메인을 구현하는 것을 고려해 보십시오. 격리 요구 사항에 따라 단일 계정 및 리전 내에서 여러 LOB(Line of Business)를 여러 도메인으로 구현할 수 있습니다. 같은 팀/LOB의 구성원 간에 거의 실시간으로 협업하려면 공유 스페이스를 사용하세요. 도메인이 여러 개인 경우에도 여전히 자격 증명 액세스 관리(IAM) 정책 및 권한을 사용하여 리소스를 격리할 수 있습니다.

도메인에서 생성된 SageMaker 리소스는 도메인 Amazon 리소스 이름(ARN)과 사용자 프로필 또는 스페이스 ARN으로 자동 태그가 지정되므로 리소스를 쉽게 격리할 수 있습니다. 샘플 정책은 도메인 리소스 격리 설명서를 참조하십시오. 여기에서 설명서의 기능 비교와 함께 다중 계정 또는 다중 도메인 전략을 사용하는 경우에 대한 자세한 참조를 볼 수 있으며 GitHub 리포지토리에서 기존 도메인의 태그를 채우는 샘플 스크립트를 볼 수 있습니다.

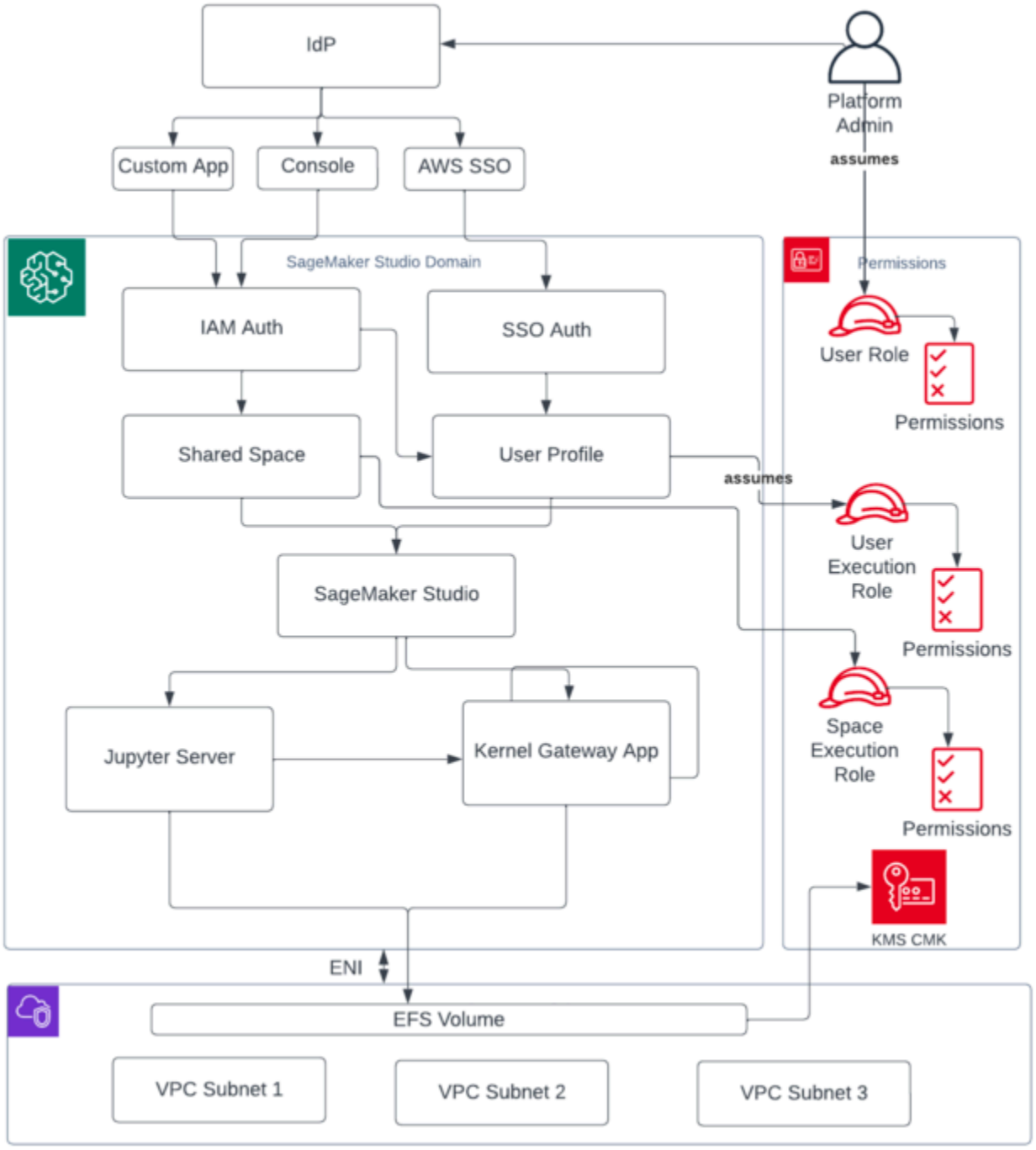
마지막으로, AWS Service Catalog를 사용하여 여러 계정에 SageMaker Studio 리소스의 셀프 서비스 배포를 구현할 수 있습니다. 자세한 내용은 다수의 AWS 계정 및 AWS 리전에서의 AWS Service Catalog 제품 관리를 참조하세요.

도메인 관리

Amazon SageMaker 도메인은 다음과 같이 구성됩니다.

- 관련된 Amazon Elastic File System(Amazon EFS) 볼륨
- 권한이 부여된 사용자 목록
- 다양한 보안, 애플리케이션, 정책 및 Amazon Virtual Private Cloud(VPC) 구성

아래 그림에는 SageMakerStudio 도메인을 구성하는 다양한 구성 요소가 종합적으로 소개되어 있습니다.

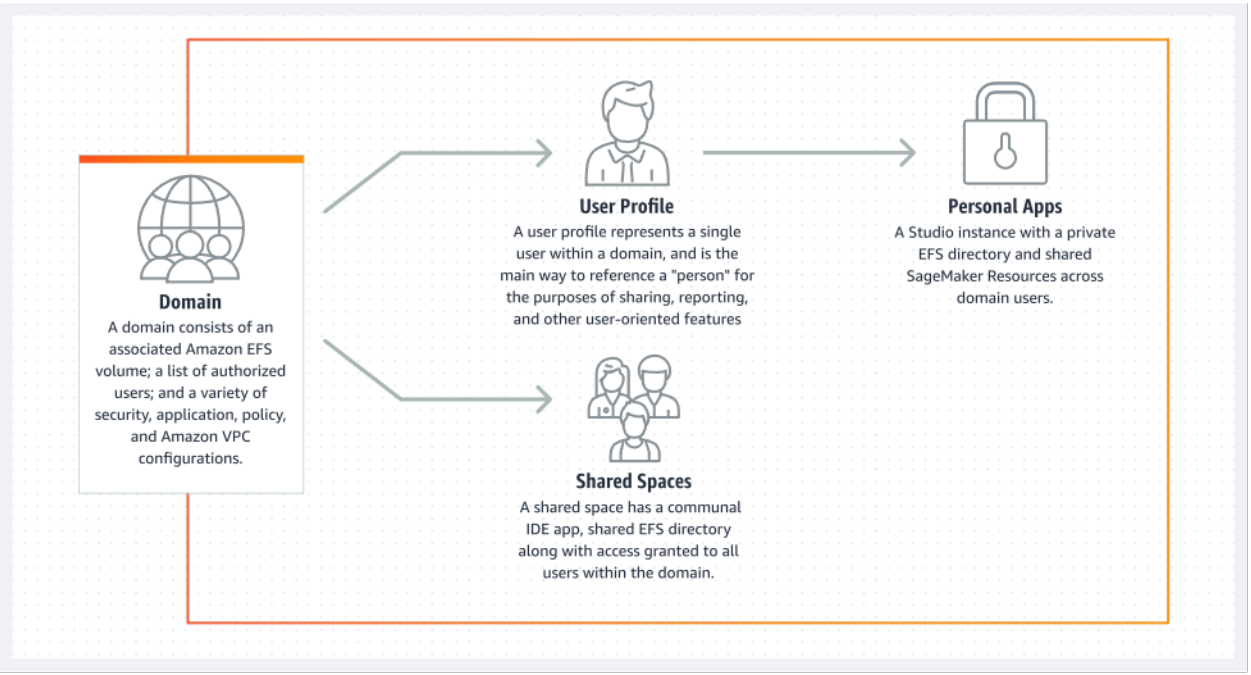


SageMaker Studio 도메인을 구성하는 다양한 구성 요소에 대한 상위 수준의 보기

다중 도메인 및 공유 스페이스

Amazon은 SageMaker 이제 각 계정에 AWS 리전 대해 하나의 SageMaker 도메인을 여러 개 생성할 수 있도록 지원합니다. 각 도메인은 인증 모드와 같은 고유한 도메인 설정과 VPC 및 서브넷과 같은 네트워킹 설정을 가질 수 있습니다. 사용자 프로필은 도메인 간에 공유할 수 없습니다. 인간 사용자가 도메인으로 분리된 여러 팀에 속해 있는 경우 각 도메인에서 해당 사용자에 대한 사용자 프로필을 생성하십시오. 기존 도메인의 태그 채우기에 대해 알아보려면 다중 도메인 개요를 참조하세요.

IAM 인증 모드로 설정된 각 도메인은 공유 스페이스를 활용하여 거의 실시간인 사용자간 협업을 수행할 수 있습니다. 공유 공간을 통해 사용자는 공유 Amazon EFS 디렉터리와 사용자 인터페이스용 공유 JupyterServer앱에 액세스하고 거의 실시간으로 공동 편집할 수 있습니다. 공유 스페이스에서 생성된 리소스의 자동 태그 지정을 통해 관리자는 프로젝트 수준에서 비용을 추적할 수 있습니다. 또한 공유 JupyterServer UI는 실험 및 모델 레지스트리 항목과 같은 리소스를 필터링하여 공유된 ML 작업과 관련된 항목만 표시되도록 합니다. 다음 다이어그램은 각 도메인 내의 비공개 앱 및 공유 스페이스에 대한 개요를 제공합니다.



단일 도메인 내의 비공개 앱 및 공유 스페이스 개요

도메인에 공유 스페이스 설정

공유 스페이스는 일반적으로 단일 도메인의 구성원이 동일한 기본 파일 저장소 및 IDE에 거의 실시간으로 액세스해야 하는 특정 ML 작업이나 프로젝트를 위해 만들어집니다. 사용자는 거의 실시간으로 노

트북에 액세스하고, 읽고, 편집하고, 공유할 수 있으므로 동료와 함께 반복 작업을 아주 빠르게 시작할 수 있습니다.

공유 스페이스를 만들려면 먼저 스페이스를 사용하는 모든 사용자의 권한을 제어할 스페이스 기본 실행 역할을 지정해야 합니다. 이 글을 쓰는 시점에서 도메인 내의 모든 사용자는 해당 도메인의 모든 공유 스페이스에 액세스할 수 있습니다. 기존 도메인에 공유 스페이스를 추가하는 방법에 대한 최신 설명서를 확인하려면 공유 공간 만들기를 참조하세요.

IAM 페더레이션을 위한 도메인 설정

SageMaker Studio 도메인에 대한 AWS Identity and Access Management (IAM) 페더레이션을 설정하기 전에 ID 관리 섹션에 설명된 대로 IdP에 IAM 페더레이션 사용자 역할 (예: 플랫폼 관리자) 을 설정해야 합니다.

IAM 옵션으로 SageMaker Studio를 설정하는 방법에 대한 자세한 지침은 IAM ID 센터를 사용하여 Amazon SageMaker 도메인에 온보딩을 참조하십시오.

Single Sign-On(SSO) 페더레이션을 위한 도메인 설정

싱글 사인온 (SSO) 페더레이션을 사용하려면 Studio를 실행해야 하는 동일한 지역의 AWS Organizations관리 AWS IAM Identity Center 계정에서 활성화해야 합니다. SageMaker 도메인 설정 단계는 인증 섹션에서 AWS IAM Identity Center(IdC)를 선택한다는 점을 제외하면 IAM 페더레이션 단계와 비슷합니다.

자세한 지침은 IAM ID 센터를 사용하여 Amazon SageMaker 도메인에 등록하기를 참조하십시오.

SageMaker 스튜디오 사용자 프로필

사용자 프로필은 도메인 내의 단일 사용자를 나타내며 공유, 보고 및 기타 사용자 중심 기능을 목적으로 “사람”을 참조하는 주된 방법입니다. 이 엔티티는 사용자가 toSageMaker Studio를 온보딩할 때 생성됩니다. 관리자가 이메일로 사용자를 초대하거나 IdC에서 가져오는 경우 사용자 프로파일이 자동으로 생성됩니다. 사용자 프로필은 개별 사용자 설정의 기본 소유자이며 사용자의 프라이빗 Amazon Elastic File System(Amazon EFS) 홈 디렉터리에 대한 참조를 포함합니다. SageMaker Studio 애플리케이션의 각 물리적 사용자에 대한 사용자 프로필을 생성하는 것이 좋습니다. 각 사용자는 Amazon EFS에 고유한 전용 디렉터리를 가지고 있으며, 사용자 프로필을 동일한 계정의 여러 도메인에서 공유할 수 없습니다.

SageMaker 스튜디오 도메인을 공유하는 각 사용자 프로필에는 노트북을 실행하기 위한 전용 컴퓨팅 리소스 (예: SageMaker Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스) 가 제공됩니다. 사용자 1에 할당된 컴퓨팅 인스턴스는 사용자 2에게 할당된 컴퓨팅 인스턴스와 완전히 분리되어 있습니다. 마찬가지로, 한 AWS 계정의 사용자들에게 할당된 컴퓨팅 리소스는 다른 계정의 사용자들에게 할당된 컴퓨팅 리소스와 완전히 분리됩니다. 각 사용자는 격리된 Docker 컨테이너 내에서 최대 4개의 애플리케이션(앱) 을 실행하거나 동일한 인스턴스 유형의 이미지를 실행할 수 있습니다.

Jupyter 서버 앱

미리 서명된 URL에 액세스하거나 AWS IAM iDC를 사용하여 로그인하여 사용자용 Amazon SageMaker Studio 노트북을 시작하면 서비스 관리형 VPC 인스턴스에서 Jupyter Server 앱이 실행됩니다. SageMaker 각 사용자는 전용 Jupyter 서버 앱을 프라이빗 앱으로 받습니다. 기본적으로 SageMaker 스튜디오 노트북용 Jupyter Server 앱은 전용 인스턴스 (시스템 인스턴스 유형으로 예약됨) 에서 실행됩니다. *ml.t3.medium* 이 인스턴스의 컴퓨팅 요금은 고객에게 청구되지 않습니다.

Jupyter 커널 게이트웨이 앱

커널 게이트웨이 앱은 API 또는 SageMaker Studio 인터페이스를 통해 생성할 수 있으며 선택한 인스턴스 유형에서 실행됩니다. 이 앱은 널리 사용되는 데이터 사이언스 및 Apache MXnet 및 같은 TensorFlow딥 러닝 패키지로 사전 구성된 기본 제공 SageMaker Studio 이미지 중 하나를 사용하여 실행할 수 있습니다. PyTorch

사용자는 동일한 Studio 이미지/커널 게이트웨이 앱 내에서 여러 Jupyter 노트북 커널, 터미널 세션 및 대화형 콘솔을 시작하고 실행할 수 있습니다. SageMaker 또한 사용자는 동일한 물리적 인스턴스에서 최대 4개의 커널 게이트웨이 앱 또는 이미지를 실행할 수 있으며 각 애플리케이션은 컨테이너/이미지로 격리됩니다.

추가 앱을 만들려면 다른 인스턴스 유형을 사용해야 합니다. 사용자 프로필에서는 인스턴스 유형에 관계없이 하나의 인스턴스만 실행할 수 있습니다. 예를 들어 사용자는 SageMaker Studio의 내장 데이터 과학 이미지를 사용하는 간단한 노트북과 내장 이미지를 사용하는 다른 노트북을 동일한 인스턴스에서 모두 실행할 수 있습니다. TensorFlow 인스턴스가 실행되는 시간만큼 사용자에게 요금이 청구됩니다. 사용자가 SageMaker Studio를 적극적으로 실행하지 않을 때 비용이 발생하지 않도록 하려면 사용자는 인스턴스를 종료해야 합니다. 자세한 내용은 Studio 앱 종료 및 업데이트를 참조하세요.

SageMaker Studio 인터페이스에서 Kernel Gateway 앱을 종료하고 다시 열 때마다 해당 앱이 새 인스턴스에서 시작됩니다. 즉, 동일한 앱을 다시 시작해도 패키지 설치가 지속되지 않습니다. 마찬가지로 사용자가 노트북에서 인스턴스 유형을 변경하면 설치된 패키지와 세션 변수가 손실됩니다. 하지

만 자체 이미지 및 라이프사이클 스크립트를 가져오는 등의 기능을 사용하여 사용자 고유의 패키지를 SageMaker Studio로 가져와서 인스턴스 전환 및 새 인스턴스 시작 시에도 유지할 수 있습니다.

Amazon Elastic File System 볼륨

도메인이 생성되면 도메인 내의 모든 사용자가 사용할 수 있는 Amazon Elastic File System(Amazon EFS) 볼륨이 하나 생성됩니다. 각 사용자 프로필은 Amazon EFS 볼륨 내에서 사용자의 노트북, GitHub 리포지토리 및 데이터 파일을 저장하는 프라이빗 홈 디렉터리를 받습니다. 도메인 내의 각 스페이스는 여러 사용자 프로필이 액세스할 수 있는 Amazon EFS 볼륨 내의 프라이빗 디렉터리를 수신합니다. 폴더에 대한 액세스는 파일 시스템 권한을 통해 사용자별로 분리됩니다. SageMaker Studio는 각 사용자 프로필 또는 스페이스에 대해 글로벌 고유 사용자 ID를 생성하고 이를 EFS의 사용자 홈 디렉터리에 대한 POSIX (휴대용 운영 체제 인터페이스) 사용자/그룹 ID로 적용하여 다른 사용자/스페이스가 해당 데이터에 액세스하는 것을 방지합니다.

백업 및 복구

기존 EFS 볼륨은 새 SageMaker 도메인에 연결할 수 없습니다. 프로덕션 설정에서 (다른 EFS 볼륨 또는 Amazon Simple Storage Service(S3)에) Amazon EFS 볼륨이 백업되었는지 확인합니다. EFS 볼륨이 실수로 삭제된 경우 관리자는 SageMaker Studio 도메인을 해체하고 다시 생성해야 합니다. 프로세스는 다음과 같습니다.

`ListUserProfiles`, `DescribeUserProfile`, `List Spaces`, 및 `DescribeSpace` API 호출을 통해 사용자 프로필, 스페이스 및 관련 EFS 사용자 ID(UID) 목록을 백업합니다.

1. 새 SageMaker Studio 도메인을 생성합니다.
2. 사용자 프로필 및 스페이스를 생성합니다.
3. 각 사용자 프로필에 대해 EFS/Amazon S3의 백업에서 파일을 복사합니다.
4. 원하는 경우 이전 SageMaker Studio 도메인에서 모든 앱과 사용자 프로필을 삭제할 수 있습니다.

자세한 지침은 부록 섹션 SageMaker Studio 도메인 백업 및 복구를 참조하십시오.

> **Note**
>
> 이는 사용자가 앱을 시작할 때마다 `LifecycleConfigurations`을 통해 S3와 데이터를 주고 받아서도 달성할 수 있습니다.

Amazon EBS 볼륨

아마존 엘라스틱 블록 스토어 (Amazon EBS) 스토리지 볼륨도 각 SageMaker 스튜디오 노트북 인스턴스에 연결됩니다. 이것은 인스턴스에서 실행되는 컨테이너 또는 이미지의 루트 볼륨으로 사용됩니다. Amazon EFS 스토리지는 영구적이지만, 컨테이너에 연결된 Amazon EBS 볼륨은 일시적입니다. 고객이 앱을 삭제하면 Amazon EBS 볼륨에 로컬로 저장된 데이터는 유지되지 않습니다.

미리 서명된 URL에 대한 액세스 보안

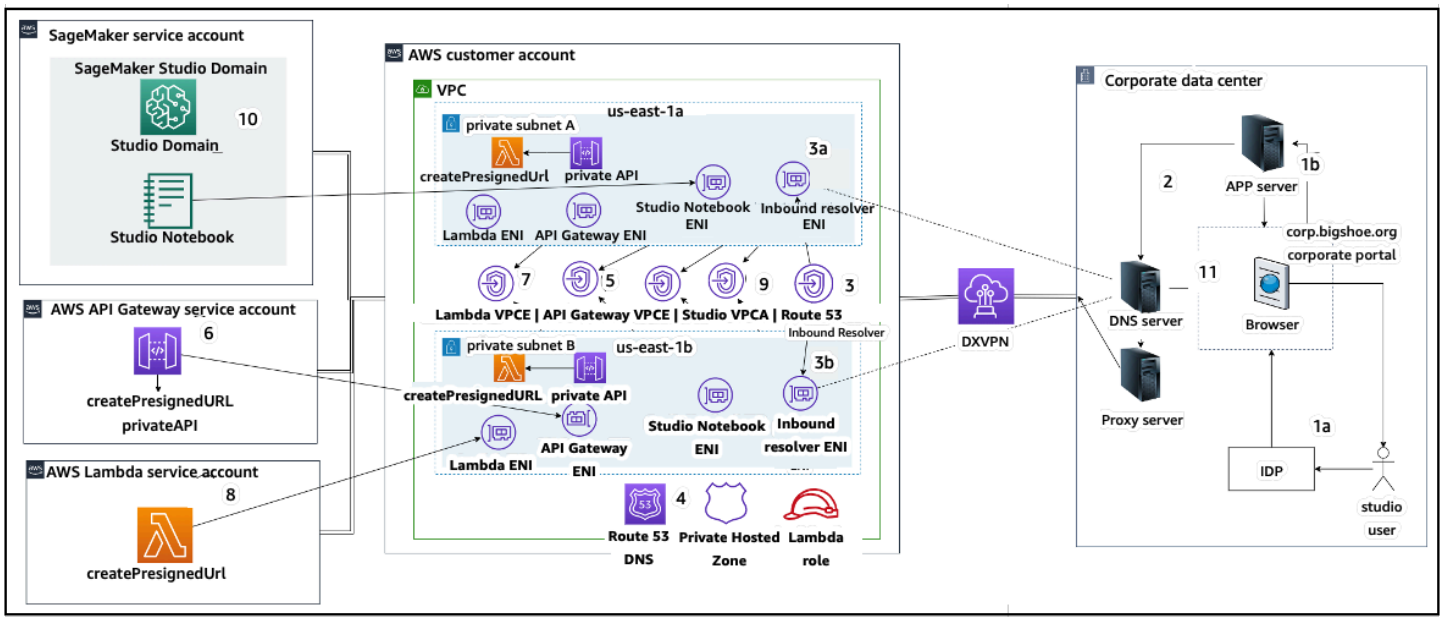
SageMaker Studio 사용자가 노트북 링크를 열면 SageMaker Studio는 연동 사용자의 IAM 정책을 검증하여 액세스를 승인하고 사용자를 위해 사전 서명된 URL을 생성 및 확인합니다. SageMaker 콘솔은 인터넷 도메인에서 실행되므로 이렇게 생성된 사전 서명된 URL은 브라우저 세션에서 볼 수 있습니다. 이로 인해 적절한 액세스 제어가 시행되지 않을 경우 데이터 도용 및 고객 데이터에 대한 액세스 권한을 획득할 수 있는 원치 않는 위협 요소가 발생할 수 있습니다.

Studio는 미리 서명된 URL 데이터 도용에 대해 액세스 제어를 적용하는 몇 가지 방법을 지원합니다.

- IAM 정책 조건 `aws:sourceIp`를 사용한 클라이언트 IP 검증
- IAM 조건 `aws:sourceVpc`를 사용한 클라이언트 VPC 검증
- IAM 정책 조건 `aws:sourceVpce`를 사용한 클라이언트 VPC 엔드포인트 검증

SageMaker콘솔에서 SageMaker Studio 노트북에 액세스할 때 사용할 수 있는 유일한 옵션은 IAM 정책 조건에 따라 클라이언트 IP 검증을 사용하는 것입니다. `aws:sourceIp` 하지만 Zscaler와 같은 브라우저 트래픽 라우팅 제품을 사용하여 작업 인력 인터넷 액세스의 규모와 규정 준수를 보장할 수 있습니다. 이러한 트래픽 라우팅 제품은 자체 소스 IP를 생성하며, 이 IP 범위는 기업 고객이 제어하지 않습니다. 따라서 이러한 기업 고객은 `aws:sourceIp` 조건을 사용할 수 없습니다.

IAM 정책 조건을 `aws:sourceVpce` 사용하여 클라이언트 VPC 엔드포인트 검증을 사용하려면 Studio가 배포된 동일한 고객 VPC에서 사전 서명된 URL을 생성해야 하며, 고객 VPC의 SageMaker Studio VPC 엔드포인트를 통해 사전 서명된 URL을 확인해야 합니다. SageMaker 기업 네트워크 사용자의 액세스 시간 동안 미리 서명된 URL의 이러한 확인은 다음 아키텍처에 표시된 것처럼 DNS 전달 규칙(Zscaler 및 기업 DNS 모두)을 사용하여 수행한 다음 Amazon Route 53 인바운드 확인자를 사용하여 고객 VPC 엔드포인트로 전송할 수 있습니다.



기업 네트워크를 통해 VPC 엔드포인트가 있는 Studio 미리 서명된 URL에 액세스

위의 아키텍처를 설정하는 방법에 대한 step-by-step 지침은 Amazon SageMaker Studio 사전 서명 URL 보안 1부: 기본 인프라를 참조하십시오.

SageMaker 도메인 할당량 및 한도

- SageMaker Studio 도메인 SSO 페더레이션은 AWS Identity Center가 제공되는 AWS 조직의 구성원 계정 전체에서 해당 지역에서만 지원됩니다.
- AWS Identity Center를 사용하여 설정된 도메인에서는 현재 공유 스페이스가 지원되지 않습니다.
- 도메인을 생성한 후에는 VPC 및 서브넷 구성을 변경할 수 없습니다. 하지만 다른 VPC 및 서브넷 구성으로 새 도메인을 생성할 수 있습니다.
- 도메인을 생성한 후에는 IAM과 SSO 모드 간에 도메인 액세스를 전환할 수 없습니다. 다른 인증 모드로 새 도메인을 생성할 수 있습니다.
- 모든 사용자에 대해 인스턴스 유형당 실행되는 커널 게이트웨이 앱은 4개로 제한됩니다.
- 각 사용자는 각 인스턴스 유형에서 하나의 인스턴스만 시작할 수 있습니다.
- 도메인 내에서 소비되는 리소스에는 제한이 있습니다(예: 인스턴스 유형별로 시작하는 인스턴스 수, 생성할 수 있는 사용자 프로필 수). 서비스 한도의 전체 목록은 서비스 할당량 페이지를 참조하십시오.
- 고객은 도메인 또는 사용자 프로필 수와 같은 기본 리소스 제한을 상향 조정하는 데 필요한 비즈니스 근거가 있는 기업 지원 사례를 제출할 수 있으며, 여기에는 계정 수준의 가드레일이 적용됩니다.

- 계정당 동시 앱 수는 앱 2,500개로 엄격히 제한됩니다. 도메인 및 사용자 프로필 한도는 이 엄격한 한도에 따라 달라집니다. 예를 들어 계정에는 1,000개의 사용자 프로필이 있는 단일 도메인 또는 각각 50개의 사용자 프로필이 있는 20개의 도메인이 있을 수 있습니다.

자격 증명 관리

이 섹션에서는 회사 디렉터리의 인력 사용자가 Studio로 AWS 계정 페더레이션하고 Studio에 액세스하는 방법을 설명합니다. SageMaker 먼저 사용자, 그룹, 역할이 매핑되는 방식과 사용자 페더레이션이 작동하는 방식을 간략하게 설명하겠습니다.

사용자, 그룹 및 역할

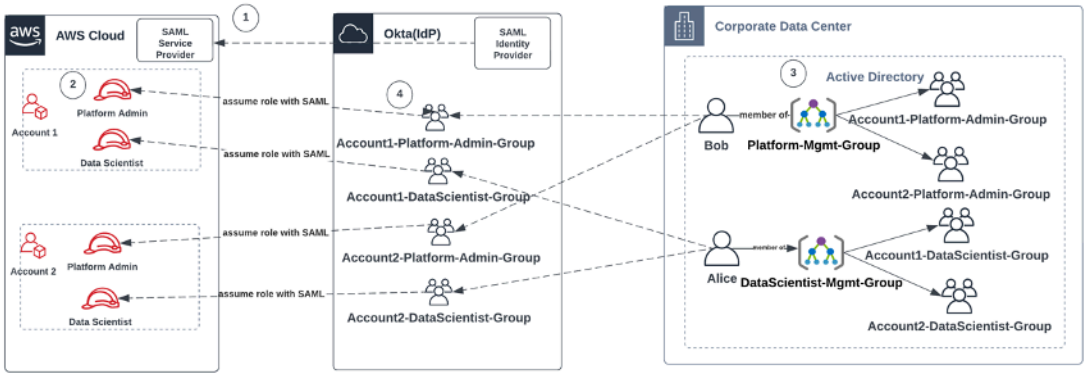
에서는 사용자 AWS, 그룹 및 역할을 사용하여 리소스 권한을 관리합니다. 고객은 IAM을 통해 또는 Active Directory(AD)와 같은 회사 디렉터리를 통해 사용자와 그룹을 관리할 수 있습니다. 이 디렉터리는 Okta와 같은 외부 IdP를 통해 활성화되어 클라우드와 온프레미스에서 실행되는 다양한 애플리케이션에 사용자를 인증할 수 있습니다.

AWS Security Pillar ID 관리 섹션에서 설명한 것처럼 중앙 IdP에서 사용자 ID를 관리하는 것이 가장 좋습니다. 이렇게 하면 백엔드 HR 프로세스와 쉽게 통합되고 직원 사용자에 대한 액세스를 관리하는 데 도움이 되기 때문입니다.

IdPs 예를 들어 Okta를 사용하면 최종 사용자가 SAML (보안 어설션 마크업 언어) 이 포함된 SSO를 사용하여 하나 이상의 사용자를AWS 계정 인증하고 특정 역할에 액세스할 수 있습니다. IdP 관리자는 AWS 계정 IdP에서 역할을 다운로드하여 사용자에게 할당할 수 있습니다. 에 AWS로그인하면 최종 사용자에게 할당된 AWS 역할 목록이 하나 이상 표시되는 AWS 화면이 표시됩니다. AWS 계정최종 사용자는 로그인할 때 맡을 역할을 선택할 수 있으며, 이 역할에 따라 인증된 세션 기간 동안의 권한이 정의됩니다.

IdP에는 액세스를 제공하려는 각 특정 계정 및 역할 조합에 대한 그룹이 존재해야 합니다. 이러한 그룹들은 AWS 역할별 그룹이라고 부르겠습니다. 이러한 역할별 그룹의 구성원인 모든 사용자에게는 한 가지 권한이 부여됩니다. 즉, 한 개의 특정 AWS 계정내에서 하나의 특정 역할에 액세스할 수 있는 것입니다. 하지만 이 단일 권한 부여 프로세스로는 각 사용자를 특정 AWS 역할 그룹에 할당하여 사용자 액세스를 관리할 수 있을 정도로 확장되지 않습니다. 관리를 단순화하려면 조직 내에서 서로 다른 AWS 권한 집합이 필요한 모든 개별 사용자 집합에 대해 여러 그룹을 만드는 것이 좋습니다.

중앙 IdP 설정을 설명하기 위해 사용자 및 그룹이 IdP 디렉터리와 동기화되는 AD 설정을 사용하는 엔터프라이즈를 예로 들어 보겠습니다. AWS에서는 이러한 AD 그룹이 IAM 역할에 매핑됩니다. 워크플로의 주요 단계는 다음과 같습니다.



AD 사용자, AD 그룹 및 IAM 역할을 온보딩하기 위한 워크플로

1. 에서 AWS각 IdP에 대해 SAML 통합을 설정합니다. AWS 계정
2. 에서 AWS각각에 역할을 설정하고 AWS 계정 IdP와 동기화합니다.
3. 기업 AD 시스템에서:
   a. 각 계정 역할에 대해 AD 그룹을 만들고 IdP에 동기화합니다 (예: (AWS 역할 그룹이라고도 함). `Account1-Platform-Admin-Group`
   b. 각 페르소나 수준 (예:`Platform-Mgmt-Group`) 에서 관리 그룹을 만들고 AWS 역할 그룹을 구성원으로 할당합니다.
   c. 해당 관리 그룹에 사용자를 할당하여 AWS 계정 역할에 대한 액세스를 허용하세요.
4. IdP에서 AWS 역할 그룹 (예:`Account1-Platform-Admin-Group`) 을 AWS 계정 역할 (예: Account1의 플랫폼 관리자) 에 매핑합니다.
5. 데이터 과학자 Alice가 Idp에 로그인하면 '계정 1 데이터 과학자'와 '계정 2 데이터 과학자' 중에서 선택할 수 있는 두 가지 옵션이 있는 AWS 페더레이션 앱 UI가 제공됩니다.
6. Alice는 'Account 1 데이터 사이언티스트' 옵션을 선택하면 Account 1 (콘솔) 의 인증된 애플리케이션에 연결됩니다. AWS SageMaker

SAML 계정 페더레이션 설정에 대한 자세한 지침은 Okta의 계정 페더레이션을 위한 SAML 2.0 구성 방법을 참조하십시오. AWS

사용자 페더레이션

SageMaker 스튜디오에 대한 인증은 IAM 또는 IAM IdC를 사용하여 수행할 수 있습니다. IAM을 통해 사용자를 관리하는 경우 사용자는 IAM 모드를 선택할 수 있습니다. 기업에서 외부 IdP를 사용하는 경

우 IAM 또는 IAM IdC를 통해 페더레이션할 수 있습니다. 기존 SageMaker Studio 도메인의 인증 모드는 업데이트할 수 없으므로 프로덕션 SageMaker Studio 도메인을 생성하기 전에 먼저 결정을 내리는 것이 중요합니다.

SageMaker Studio가 IAM 모드로 설정된 경우 SageMaker Studio 사용자는 브라우저를 통해 Studio 앱에 액세스할 때 SageMaker Studio 앱에 자동으로 로그인하는 미리 서명된 URL을 통해 앱에 액세스합니다.

IAM 사용자

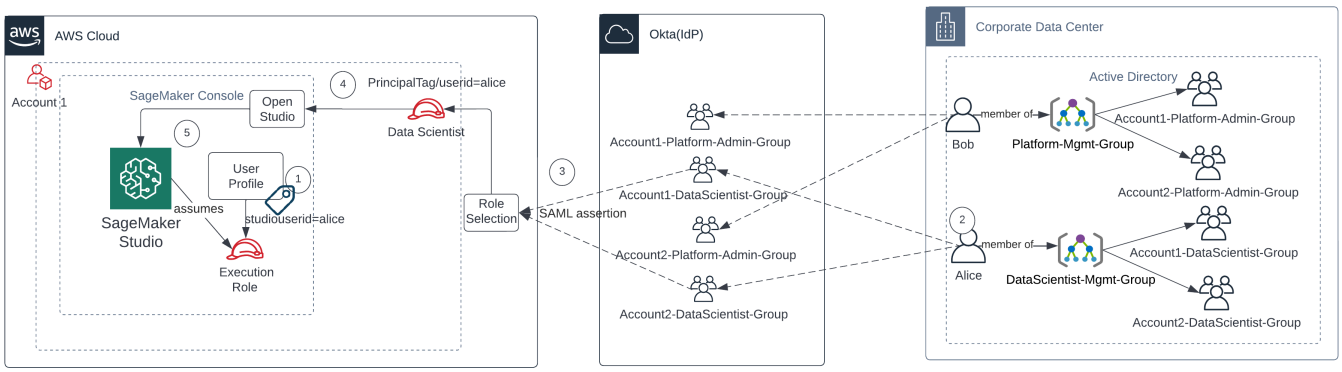
IAM 사용자의 경우 관리자는 각 사용자에 대한 SageMaker Studio 사용자 프로필을 생성하고 이 사용자 프로필을 IAM 역할과 연결하여 사용자가 Studio 내에서 수행해야 하는 필수 작업을 수행할 수 있도록 합니다. 사용자가 자신의 SageMaker Studio AWS 사용자 프로필에만 액세스하는 것을 제한하려면 관리자는 SageMaker Studio 사용자 프로필에 태그를 지정하고 태그 값이 사용자 이름과 동일한 경우에만 액세스를 허용하는 IAM 정책을 사용자에게 첨부해야 합니다. AWS 정책 명령문은 다음과 같습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:username}"
                }
            }
        }
    ]
}
```

AWS IAM 또는 계정 페더레이션

AWS 계정 페더레이션 방법을 사용하면 고객이 Okta와 같은 SAML IdP에서 SageMaker 콘솔로 페더레이션할 수 있습니다. 사용자가 자신의 사용자 프로필에만 액세스하는 것을 제한하려면 관리자는

SageMaker Studio 사용자 `PrincipalTags` 프로필에 태그를 지정하고 IdP를 추가한 다음 이를 전이적 태그로 설정해야 합니다. 다음 다이어그램은 연동 사용자 (데이터 과학자 앨리스) 가 자신의 Studio 사용자 프로필에 액세스할 수 있는 권한을 부여하는 방법을 보여줍니다. SageMaker



IAM SageMaker 페더레이션 모드에서 스튜디오에 액세스

1. Alice SageMaker Studio 사용자 프로필에는 사용자 ID로 태그가 지정되며 실행 역할과 연결됩니다.
2. Alice가 IdP(Okta)에 인증합니다.
3. IdP는 Alice를 인증하고 Alice가 속한 두 역할(계정 1과 2의 경우 데이터 과학자)과 함께 SAML 어설션을 게시합니다. Alice는 계정 1의 데이터 과학자 역할을 선택합니다.
4. Alice는 데이터 과학자 역할을 맡아 계정 1 SageMaker 콘솔에 로그인했습니다. Alice는 Studio 앱 인스턴스 목록에서 Studio 앱 인스턴스를 엽니다.
5. 위임된 역할 세션의 Alice 주 태그는 선택한 SageMaker Studio 앱 인스턴스 사용자 프로필 태그와 비교하여 검증됩니다. 프로필 태그가 유효하면 실행 역할을 맡아 SageMaker Studio 앱 인스턴스가 시작됩니다.

사용자 온보딩의 일환으로 SageMaker 실행 역할 및 정책 생성을 자동화하려는 경우 다음과 같은 방법으로 이를 수행할 수 있습니다.

1. 예를 들어 각 계정 및 Studio 도메인 수준에서 AD 그룹(예: `SageMaker-Account1-Group`)을 설정합니다.
2. 사용자를 Studio에 온보딩해야 하는 경우 사용자의 SageMaker 그룹 구성원에 -Account1-Group을 추가하십시오. SageMaker

`SageMaker-Account1-Group`멤버십 이벤트를 수신하는 자동화 프로세스를 설정하고 AWS API를 사용하여 AD 그룹 멤버십을 기반으로 역할, 정책, 태그 및 SageMaker Studio 사용자 프로필을 생성합

니다. 해당 역할을 사용자 프로파일에 추가합니다. 샘플 정책은 을 참조하십시오. SageMaker Studio 사용자가 다른 사용자 프로필에 접근하지 못하도록 방지

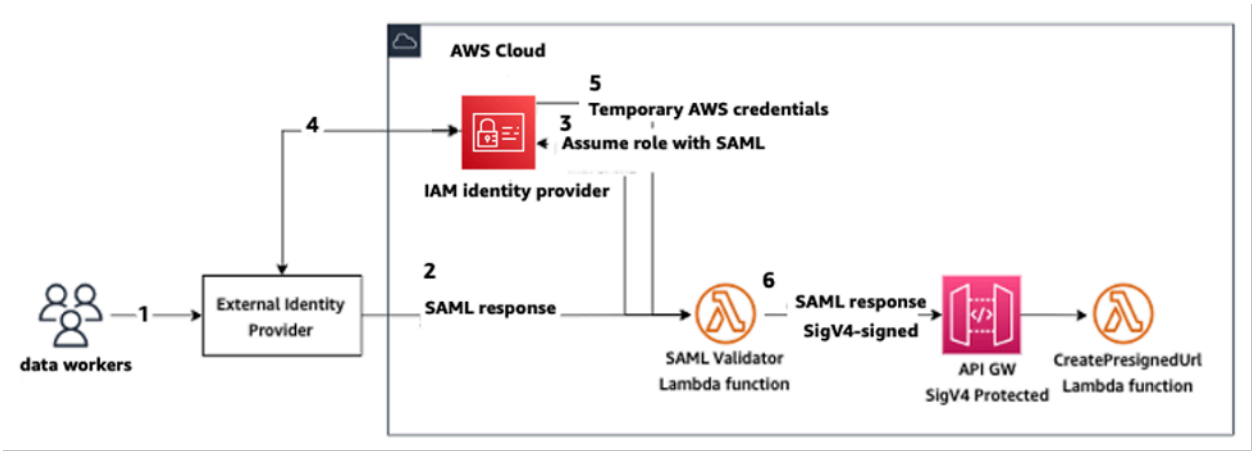
SAML 인증: 사용 AWS Lambda

IAM 모드에서는 SAML 어설션을 사용하여 SageMaker Studio에 사용자를 인증할 수도 있습니다. 이 아키텍처에서 고객은 기존 IdP를 사용하여 사용자가 Studio에 액세스할 수 있도록 SAML 애플리케이션을 생성할 수 있습니다 (AWS ID 페더레이션 애플리케이션 대신). 고객의 IdP는 IAM에 추가됩니다. AWS Lambda 함수는 IAM 및 STS를 사용하여 SAML 어설션을 검증한 다음 API 게이트웨이 또는 Lambda 함수를 직접 호출하여 사전 서명된 도메인 URL을 생성합니다.

이 솔루션의 장점은 Lambda 함수가 Studio에 액세스하기 위한 로직을 사용자 지정할 수 있다는 것입니다. SageMaker 예:

- 사용자 프로필이 없는 경우에는 사용자 프로필을 자동으로 생성합니다.
- SAML 속성을 파싱하여 역할 또는 정책 문서를 SageMaker Studio 실행 역할에 연결하거나 제거합니다.
- 생명 주기 구성(LCC)을 추가하고 태그를 추가하여 사용자 프로필을 사용자 지정합니다.

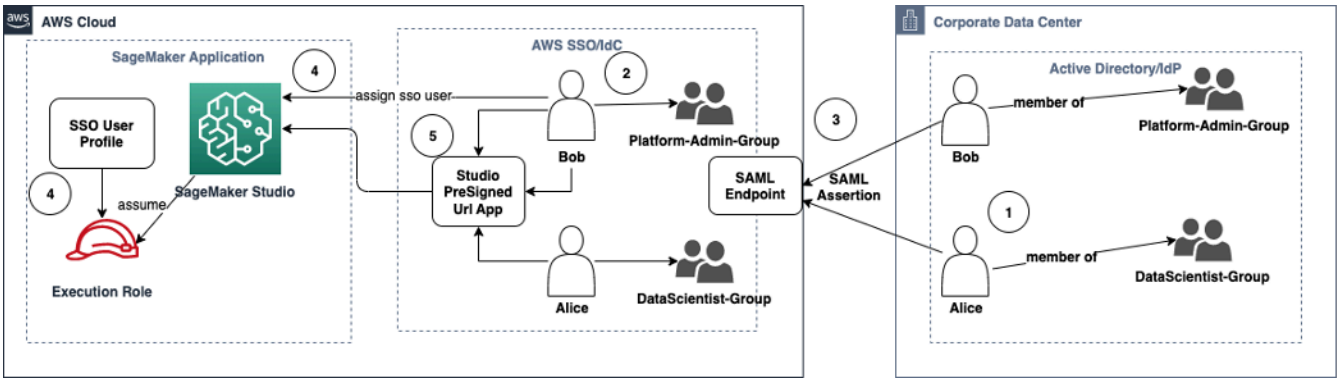
요약하면 이 솔루션은 SageMaker Studio를 인증 및 권한 부여를 위한 사용자 지정 로직이 있는 SAML2.0 애플리케이션으로 노출합니다. 구현 세부 정보는 부록 섹션 SageMaker SAML 어설션을 사용한 스튜디오 액세스를 참조하십시오.



사용자 지정 SageMaker SAML 애플리케이션을 사용하여 스튜디오에 액세스하는 방법

AWS IAM IdC 페더레이션

IdC 페더레이션 방법을 사용하면 고객이 SAML IdP (예: Okta) 에서 SageMaker 스튜디오 애플리케이션으로 직접 페더레이션할 수 있습니다. 다음 다이어그램은 연동 사용자가 자신의 Studio 인스턴스에 액세스할 수 있는 권한을 부여하는 방법을 보여줍니다. SageMaker



IAM iDC SageMaker 모드에서 스튜디오에 액세스하기

1. 기업 AD에서 사용자는 플랫폼 관리자 그룹 및 데이터 과학자 그룹과 같은 AD 그룹의 구성원입니다.
2. ID 공급자 (IdP) 의 AD 사용자 및 AD 그룹은 AWS IAM Identity Center에 동기화되며 할당을 위해 각각 싱글 사인온 사용자 및 그룹으로 사용할 수 있습니다.
3. IdP는 SAML 어설션을 iDC SAML 엔드포인트에 게시합니다. AWS
4. SageMaker 스튜디오에서는 iDC 사용자가 스튜디오 애플리케이션에 할당됩니다. SageMaker 이 할당은 iDC 그룹을 사용하여 수행할 수 있으며 SageMaker Studio는 각 IdC 사용자 수준에 적용됩니다. 이 할당이 생성되면 SageMaker Studio는 IdC 사용자 프로필을 생성하고 도메인 실행 역할을 연결합니다.
5. 사용자는 iDC에서 클라우드 애플리케이션으로 호스팅되는 미리 서명된 안전한 URL을 사용하여 SageMaker Studio 애플리케이션에 액세스합니다. SageMaker Studio는 IdC 사용자 프로필에 첨부된 실행 역할을 맡습니다.

도메인 인증 지침

도메인의 인증 모드를 선택할 때 고려해야 할 몇 가지 사항은 다음과 같습니다.

1. 사용자가 SageMaker Studio UI에 직접 AWS Management Console 액세스하여 볼 수 없게 하려면 IAM IdC에서 싱글 사인온 모드를 사용하십시오. AWS

2. 사용자가 IAM 모드에서 직접 SageMaker Studio UI에 액세스하여 볼 수 없게 하려면 백엔드에서 Lambda 함수를 사용하여 사용자 프로필에 미리 서명된 URL을 생성하고 Studio UI로 리디렉션하면 됩니다. AWS Management Console SageMaker
3. IdC 모드에서는 각 사용자가 단일 사용자 프로필에 매핑됩니다.
4. IdC 모드에서는 모든 사용자 프로필에 기본 실행 역할이 자동으로 할당됩니다. 사용자에게 다른 실행 역할을 할당하려면 API를 사용하여 사용자 프로필을 업데이트해야 합니다. UpdateUserProfile
5. 생성된 미리 서명된 URL을 사용하여 IAM 모드에서 SageMaker Studio UI 액세스를 인터넷을 통과하지 않고 VPC 엔드포인트로 제한하려는 경우 사용자 지정 DNS 확인자를 사용할 수 있습니다. 안전한 Amazon SageMaker Studio 사전 서명 URL 1부: 기본 인프라 블로그 게시물을 참조하십시오.

권한 관리

이 섹션에서는 SageMaker Studio 도메인을 프로비저닝하고 운영하기 위해 일반적으로 사용되는 IAM 역할, 정책 및 가드레일을 설정하는 모범 사례를 설명합니다.

IAM 역할 및 정책

ML 수명 주기에서 보안 주체라고 부르는 관련 사용자 및 애플리케이션을 먼저 파악하고, 이들에게 부여해야 하는 AWS 권한을 파악하는 것이 가장 좋습니다. SageMaker는 관리형 서비스이므로, 사용자를 대신하여 API 직접 호출을 할 수 있는 AWS 서비스인 서비스 보안 주체도 고려해야 합니다. 다음 다이어그램은 조직 내의 다양한 페르소나에 따라 생성하려는 다양한 IAM 역할을 보여줍니다.

SageMaker IAM 역할

이러한 역할들은 필요한 특정 IAM 권한의 몇 가지 예와 함께 자세히 설명하겠습니다.

- ML 관리자 역할 — 이 관리자는 스튜디오 도메인 및 사용자 프로필(`sagemaker:CreateDomain`,`sagemaker:CreateUserProfile`) 생성, 사용자용 AWS Key Management Service(AWS KMS) 키 생성, 데이터 과학자용 S3 버킷 생성, 컨테이너를 보관할 Amazon ECR 리포지토리 생성 등 데이터 과학자를 위한 환경을 프로비저닝하는 보안 주체입니다. 또한 사용자를 위한 기본 구성 및 수명 주기 스크립트를 설정하고, 사용자 지정 이미지를 빌드하여 SageMaker Studio 도메인에 연결하고, 사용자 지정 프로젝트, Amazon EMR 템플릿과 같은 서비스 카탈로그 제품을 제공할 수 있습니다.

  예를 들어 이 보안 주체는 훈련 작업을 실행하지 않으므로 SageMaker 훈련 또는 처리 작업을 시작할 수 있는 권한이 필요하지 않습니다. CloudFormation 또는 Terraform과 같은 인프라를 코드 템플릿으로 사용하여 도메인과 사용자를 프로비저닝하는 경우, 프로비저닝 서비스는 관리자를 대신하여 리소스를 생성하는 이 역할을 맡습니다. 이 역할은 AWS Management Console를 사용하는 SageMaker에 대한 읽기 전용 액세스 권한이 있을 수 있습니다.

  또한 이 사용자 역할에는 프라이빗 VPC 내에서 도메인을 시작하기 위한 특정 EC2 권한, EFS 볼륨을 암호화하기 위한 KMS 권한, Studio(`iam:CreateServiceLinkedRole`)에 대한 서비스 연결 역

할을 생성할 수 있는 권한이 필요합니다. 이러한 세분화된 권한에 대해서는 이 문서의 뒷부분에서 설명하겠습니다.

- 데이터 과학자 사용자 역할 — 이 보안 주체는 사용자가 SageMaker Studio에 로그인하고, 데이터를 탐색하고, 처리 및 훈련 작업 및 파이프라인을 생성하는 등의 작업을 수행합니다. 사용자에게 필요한 기본 권한은 SageMaker Studio를 시작할 수 있는 권한이며, 나머지 정책은 SageMaker 실행 서비스 역할로 관리할 수 있습니다.
- SageMaker 실행 서비스 역할 - SageMaker는 관리형 서비스이므로 사용자를 대신하여 작업을 시작합니다. 많은 고객이 훈련 작업, 처리 작업 또는 모델 호스팅 작업을 실행할 때 단일 실행 역할을 사용하기로 선택하기 때문에 이 역할은 허용되는 권한 측면에서 가장 광범위한 경우가 많습니다. 쉽게 시작할 수 있는 방법이긴 하지만, 고객의 여정이 성숙해지기 때문에 노트북 실행 역할을 API 작업에 따라 별도의 역할로 나누는 경우가 많습니다. 특히 배포된 환경에서 해당 작업을 실행하는 경우에는 더욱 그렇습니다.

  역할 생성 시 SageMaker Studio 도메인과 역할을 연결합니다. 그러나 고객은 도메인의 다양한 사용자 프로필에 서로 다른 역할을 연결할 수 있는 유연성이 필요할 수 있으므로(예: 직무에 따라) 개별 IAM 역할을 각 사용자 프로필에 연결할 수도 있습니다. 단일 실제 사용자를 단일 사용자 프로필에 매핑하는 것이 좋습니다. 사용자 프로필 생성 시 역할을 연결하지 않는 경우 기본 동작은 SageMakerStudio 도메인 실행 역할도 사용자 프로필과 연결하는 것입니다.

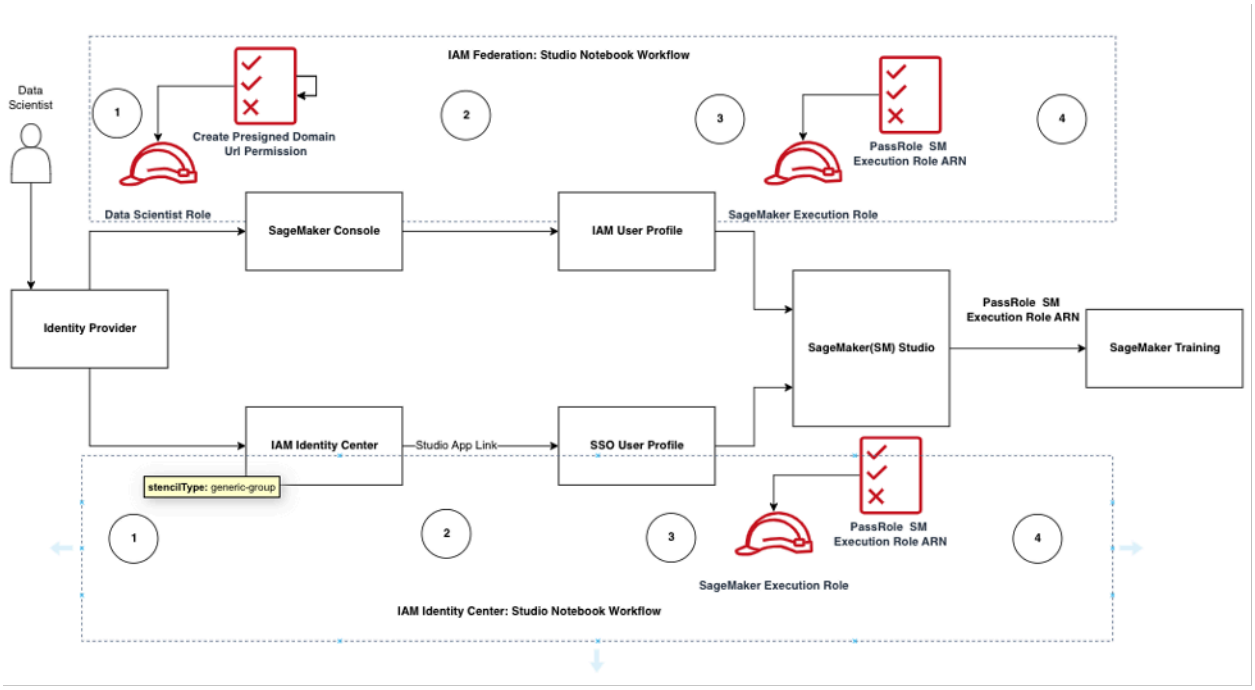
  여러 데이터 과학자와 ML 엔지니어가 프로젝트에서 함께 작업하고 리소스에 액세스하기 위한 공유 권한 모델이 필요한 경우 팀 구성원 간에 IAM 권한을 공유할 수 있는 팀 수준의 SageMaker 서비스 실행 역할을 생성하는 것이 좋습니다. 각 사용자 수준에서 권한을 잠가야 하는 경우 개별 사용자 수준 SageMaker 서비스 실행 역할을 생성할 수 있지만 서비스 한도를 염두에 두어야 합니다.

SageMaker Studio 노트북 인증 워크플로

이 섹션에서는 데이터 과학자가 SageMaker Studio 노트북에서 바로 모델을 구축하고 훈련하기 위해 수행해야 하는 다양한 활동에 대해 SageMaker Studio 노트북 인증이 어떻게 작동하는지 설명합니다. SageMaker 도메인은 두 가지 인증 모드를 지원합니다.

- IAM 페더레이션
- IAM Identity Center

다음으로 이 백서에서는 각 모드에 대한 데이터 과학자 인증 워크플로를 안내합니다.



Studio 사용자를 위한 인증 및 권한 부여 워크플로

IAM 페더레이션: SageMaker Studio 노트북 워크플로

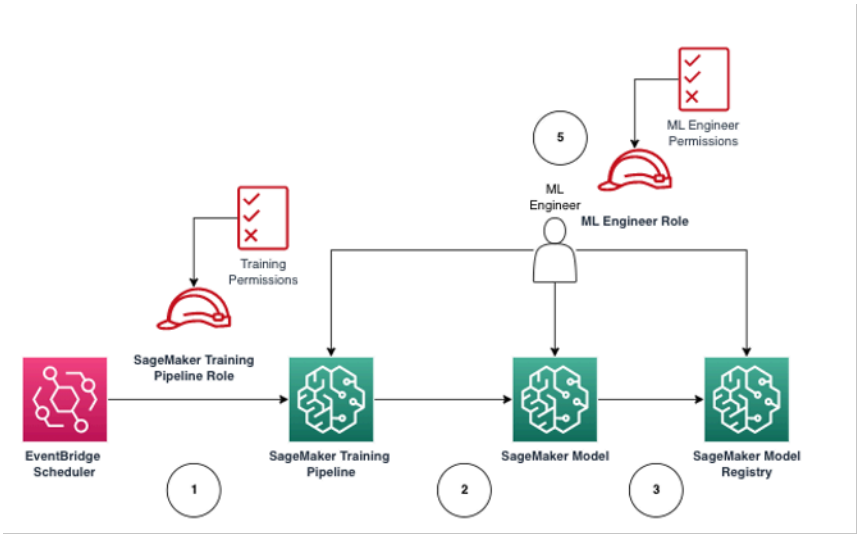
1. 데이터 과학자는 기업 ID 제공업체를 인증하고 SageMaker 콘솔에서 데이터 과학자 사용자 역할(사용자 페더레이션 역할)을 맡습니다. 이 페더레이션 역할에는 SageMaker 실행 역할에 대한 `iam:PassRole` API 권한이 있어 SageMaker Studio에 역할 Amazon 리소스 이름(ARN)을 전달할 수 있습니다.
2. 데이터 과학자는 SageMaker 실행 역할과 연결된 Studio IAM 사용자 프로필에서 Open Studio 링크를 선택합니다.
3. 사용자 프로필의 SageMaker 실행 역할 권한을 가정하여 SageMaker Studio IDE 서비스가 시작됩니다. 이 역할에는 SageMaker 실행 역할에 대한 `iam:PassRole` API 권한이 있어 역할 ARN을 SageMaker 훈련 서비스에 전달할 수 있습니다.
4. 데이터 과학자가 원격 컴퓨팅 노드에서 훈련 작업을 시작하면 SageMaker 실행 역할 ARN이 SageMaker 훈련 서비스에 전달됩니다. 그러면 이 ARN으로 새 역할 세션이 생성되고 훈련 작업이 실행됩니다. 훈련 작업에 대한 권한 범위를 더 좁혀야 하는 경우 훈련 관련 역할을 만들고 훈련 API를 직접 호출할 때 해당 역할 ARN을 전달하면 됩니다.

IAM Identity Center: SageMaker Studio 노트북 워크플로

1. 데이터 과학자는 기업 ID 제공업체를 인증하고 AWS IAM Identity Center를 클릭합니다. 데이터 과학자에게는 사용자를 위한 Identity Center 포털이 제공됩니다.
2. 데이터 과학자는 SageMaker 실행 역할과 연결된 IdC 사용자 프로필에서 생성된 SageMaker Studio 앱 링크를 클릭합니다.
3. 사용자 프로필의 SageMaker 실행 역할 권한을 가정하여 SageMaker Studio IDE 서비스가 시작됩니다. 이 역할에는 SageMaker 실행 역할에 대한 `iam:PassRole` API 권한이 있어 역할 ARN을 SageMaker 훈련 서비스에 전달할 수 있습니다.
4. 데이터 과학자가 원격 컴퓨팅 노드에서 훈련 작업을 시작하면 SageMaker 실행 역할 ARN이 SageMaker 훈련 서비스에 전달됩니다. 실행 역할 ARN은 이 ARN으로 새 역할 세션을 생성하고 훈련 작업을 실행합니다. 훈련 작업에 대한 권한 범위를 더 좁혀야 하는 경우 훈련 관련 역할을 만들고 훈련 API를 호출할 때 해당 역할 ARN을 전달하면 됩니다.

배포 환경: SageMaker 훈련 워크플로

시스템 테스트 및 프로덕션과 같은 배포된 환경에서 작업은 자동화된 스케줄러 및 이벤트 트리거를 통해 실행되며 SageMaker Studio 노트북에서는 이러한 환경에 대한 사람의 접근이 제한됩니다. 이 섹션에서는 배포된 환경에서 IAM 역할이 SageMaker 훈련 파이프라인과 함께 작동하는 방식을 설명합니다.



관리형 프로덕션 환경에서의 SageMaker 훈련 워크플로

1. Amazon EventBridge 스케줄러는 SageMaker 훈련 파이프라인 작업을 트리거합니다.

2. SageMaker 훈련 파이프라인 작업은 모델을 훈련하는 SageMaker 교육 파이프라인 역할을 맡습니다.
3. 훈련된 SageMaker 모델은 SageMaker 모델 레지스트리에 등록됩니다.
4. ML 엔지니어는 훈련 파이프라인 및 SageMaker 모델을 관리하는 ML 엔지니어 사용자 역할을 맡습니다.

데이터 권한

SageMaker Studio 사용자가 모든 데이터 소스에 액세스할 수 있는 기능은 SageMaker IAM 실행 역할과 관련된 권한에 의해 관리됩니다. 첨부된 정책을 통해 특정 Amazon S3 버킷 또는 접두사에서 읽기, 쓰기 또는 삭제하고 Amazon RDS 데이터베이스에 연결할 수 있는 권한을 부여할 수 있습니다.

AWS Lake Formation 데이터 액세스

많은 기업에서 사용자가 세밀하게 데이터에 액세스할 수 있도록 AWS Lake Formation에 의해 관리되는 데이터 레이크를 사용하기 시작했습니다. 이러한 관리 대상 데이터의 예로, 관리자는 일부 사용자의 민감한 열을 마스킹하면서도 동일한 기본 테이블에 대한 쿼리를 계속 사용할 수 있습니다.

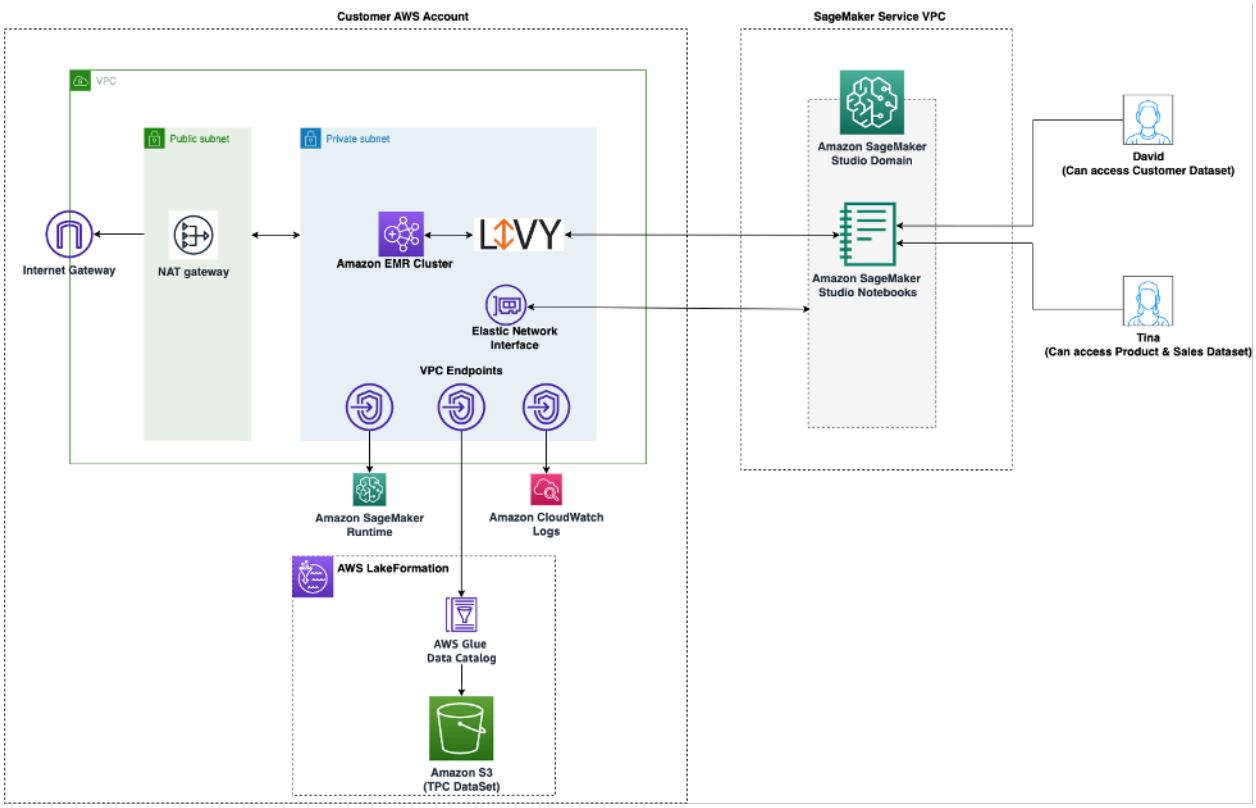
관리자는 SageMaker Studio의 Lake Formation을 활용하기 위해 SageMaker IAM 실행 역할을 `DataLakePrincipals`로 등록할 수 있습니다. 자세한 내용은 Lake Formation 권한 참조 섹션을 참조하세요. 일단 승인되면 SageMaker Studio에서 관리되는 데이터에 액세스하고 이를 작성할 수 있는 세 가지 기본 방법이 있습니다.

1. SageMaker Studio 노트북에서 사용자는 Amazon Athena와 같은 쿼리 엔진이나 boto3 위에 구축된 라이브러리를 활용하여 노트북으로 직접 데이터를 가져올 수 있습니다. Pandas용 SDK(이전에는 awswrangler로 알려짐)는 널리 사용되는 라이브러리입니다. 다음은 얼마나 원활할 수 있는지를 보여주는 코드 예제입니다.

```
transaction_id = wr.lakeformation.start_transaction(read_only=True)
df = wr.lakeformation.read_sql_query(
    sql=f"SELECT * FROM {table};",
    database=database,
    transaction_id=transaction_id
)
```

2. SageMaker Studio와 Amazon EMR의 네이티브 연결을 사용하여 대규모로 데이터를 읽고 쓸 수 있습니다. SageMaker Studio는 Apache Livy와 Amazon EMR 런타임 역할을 사용하여 SageMaker 실

행 IAM 역할(또는 기타 승인된 역할)을 Amazon EMR 클러스터로 전달하여 데이터 액세스 및 처리를 수행할 수 있는 기본 연결 기능을 구축했습니다. 최신 지침은 스튜디오에서 Amazon EMR 클러스터에 연결을 참조하세요.



SageMaker Studio의 Lake Formation에서 관리하는 데이터에 액세스하기 위한 아키텍처

3. AWS Glue 대화형 세션에 대한 SageMaker Studio 기본 연결 기능을 사용하여 대규모로 데이터를 읽고 쓸 수 있습니다. SageMaker Studio 노트북에는 AWS Glue에서 사용자가 대화형 방식으로 명령을 실행할 수 있는 커널이 내장되어 있습니다. 이를 통해 관리되는 데이터 소스에서 대규모로 데이터를 원활하게 읽고 쓸 수 있는 Python, Spark 또는 Ray 백엔드를 확장 가능하게 사용할 수 있습니다. 커널을 통해 사용자는 SageMaker 실행 또는 기타 승인된 IAM 역할을 전달할 수 있습니다. 자세한 내용은 AWS Glue 대화형 세션을 사용하여 데이터 준비를 참조하세요.

일반 가드레일

이 섹션에서는 IAM 정책, 리소스 정책, VPC 엔드포인트 정책, 서비스 제어 정책(SCP) 을 사용하여 ML 리소스에 거버넌스를 적용할 때 가장 일반적으로 사용되는 가드레일에 대해 설명합니다.

특정 인스턴스로 노트북 액세스 제한

이 서비스 제어 정책은 Studio 노트북을 만드는 동안 데이터 과학자가 액세스할 수 있는 인스턴스 유형을 제한하는 데 사용할 수 있습니다. 참고로 모든 사용자는 SageMaker Studio를 호스팅하는 기본 Jupyter 서버 앱을 만들 수 있는 “시스템” 인스턴스가 필요합니다.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "LimitInstanceTypesforNotebooks",
             "Effect": "Deny",
             "Action": [
                 "sagemaker:CreateApp"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringNotLike": {
                     "sagemaker:InstanceTypes": [
                         "ml.c5.large",
                         "ml.m5.large",
                         "ml.t3.medium",
                         "system"
                     ]
                 }
             }
         }
     ]
 }
```

규정을 준수하지 않는 SageMaker Studio 도메인 제한

SageMaker Studio 도메인의 경우 다음 서비스 제어 정책을 사용하여 고객 리소스에 액세스하는 트래픽을 강제 실행하여 해당 리소스가 퍼블릭 인터넷을 거치지 않고 고객의 VPC를 통과하도록 할 수 있습니다.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {   "Sid": "LockDownStudioDomain",
             "Effect": "Deny",
```

```
            "Action": [
                "sagemaker:CreateDomain"
            ],
            "Resource": "*",
            "Condition": {
                        "StringNotEquals": {"sagemaker:AppNetworkAccessType":
 "VpcOnly"
                },
                "Null": {
                        "sagemaker:VpcSubnets": "true",
                        "sagemaker:VpcSecurityGroupIds": "true"
                }
            }
        }
    ]
 }
```

승인되지 않은 SageMaker 이미지 실행 제한

다음 정책은 사용자가 자신의 도메인 내에서 승인되지 않은 SageMaker 이미지를 시작하는 것을 금지합니다.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "sagemaker:CreateApp"
              ],
             "Effect": "Allow",
             "Resource": "*",
             "Condition": {
                 "ForAllValues:StringNotLike": {
                     "sagemaker:ImageArns":
                         [
                         "arn:aws:sagemaker:*:*:image/{ImageName}"
                         ]
                 }
             }
         }
     ]
 }
```

SageMaker VPC 엔드포인트를 통해서만 노트북을 실행할 수 있습니다.

SageMaker는 SageMaker 컨트롤 플레인의 VPC 엔드포인트 외에도 사용자가 SageMaker Studio 노트북 또는 SageMaker 노트북 인스턴스에 연결할 수 있는 VPC 엔드포인트를 지원합니다. SageMaker Studio/노트북 인스턴스에 대한 VPC 엔드포인트를 이미 설정한 경우, 다음 IAM 조건 키는 SageMaker Studio VPC 엔드포인트 또는 SageMaker API 엔드포인트를 통해 만든 경우에만 SageMaker Studio 노트북으로의 연결을 허용합니다.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "EnableSageMakerStudioAccessviaVPCEndpoint",
             "Effect": "Allow",
             "Action": [
                 "sagemaker:CreatePresignedDomainUrl",
                 "sagemaker:DescribeUserProfile"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringEquals": {
                     "aws:sourceVpce": [
                         "vpce-111bbccc",
                         "vpce-111bbddd"
                     ]
                 }
             }
         }
     ]
 }
```

SageMaker Studio 노트북 액세스를 제한된 IP 범위로 제한

기업은 종종 SageMaker Studio 액세스를 허용된 특정 기업 IP 범위로 제한합니다. `SourceIP` 조건 키가 포함된 다음 IAM 정책은 이를 제한할 수 있습니다.

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

```
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl",
                "sagemaker:DescribeUserProfile"
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            }
        }
    ]
}
```

SageMaker Studio 사용자가 다른 사용자 프로필에 접근하지 못하도록 방지

관리자는 사용자 프로필을 생성할 때 프로필에 태그 키 `studiouserid`가 있는 SageMaker Studio 사용자 이름 태그가 지정되어 있는지 확인하십시오. 보안 주체(사용자에게 연결된 사용자 또는 역할)도 `studiouserid` 키가 있는 태그를 가져야 합니다(이 태그의 이름은 무엇이든 지정할 수 있으며 `studiouserid`에 국한되지 않음).

다음으로 SageMaker Studio를 시작할 때 사용자가 맡게 될 역할에 다음 정책을 연결합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:PrincipalTag/
studiouserid}"
                }
            }
```

```
        }
    ]
}
```

태그 지정 적용

데이터 과학자는 SageMaker Studio 노트북을 사용하여 데이터를 탐색하고 모델을 구축 및 훈련해야 합니다. 노트북에 태그를 적용하면 사용량을 모니터링하고 비용을 제어할 수 있을 뿐만 아니라 소유권 및 감사 가능성을 보장하는 데도 도움이 됩니다.

SageMaker Studio 앱의 경우 사용자 프로필에 태그가 지정되어 있는지 확인하십시오. 태그는 사용자 프로필에서 앱에 자동으로 전파됩니다. 태그를 사용하여 사용자 프로필 생성을 강제 적용하려면(CLI 및 SDK를 통해 지원됨) 관리자 역할에 다음 정책을 추가하는 것이 좋습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceUserProfileTags",
            "Effect": "Allow",
            "Action": "sagemaker:CreateUserProfile",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

훈련 작업 및 처리 작업과 같은 기타 리소스의 경우 다음 정책을 사용하여 태그를 필수로 설정할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceTagsForJobs",
            "Effect": "Allow",
```

```
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateProcessingJob",
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

SageMaker Studio의 루트 액세스

SageMaker Studio에서 노트북은 기본적으로 호스트 인스턴스에 대한 루트 액세스 권한이 없는 Docker 컨테이너에서 실행됩니다. 마찬가지로 기본 계정 실행 사용자를 제외하고 컨테이너 내의 다른 모든 사용자 ID 범위는 호스트 인스턴스 자체에서 권한이 없는 사용자 ID로 다시 매핑됩니다. 따라서 권한 상승 위협은 노트북 컨테이너 자체로 제한됩니다.

사용자 지정 이미지를 만들 때는 루트 이외의 권한을 사용자에게 제공하여 더 엄격한 제어(예: 루트 권한으로 원치 않는 프로세스를 실행하지 않도록 하거나 공개적으로 사용 가능한 패키지를 설치하는 등)를 하는 것이 좋습니다. 이 경우 Dockerfile 내에서 루트 사용자가 아닌 사용자로 실행할 이미지를 만들 수 있습니다. 사용자를 루트로 생성하든 비루트로 생성하든 관계없이 사용자의 UID/GID가 사용자 지정 앱용 AppImageConfig에 있는 UID/GID와 동일한지 확인해야 합니다. 그러면 사용자 지정 이미지를 사용하여 앱을 실행하도록 SageMaker의 구성이 생성됩니다. 예를 들어, Dockerfile이 다음과 같이 루트 사용자가 아닌 사용자를 위해 구축된 경우:

```
ARG NB_UID="1000"
ARG NB_GID="100"
...
USER $NB_UID
```

`AppImageConfig` 파일은 파일의 `KernelGatewayConfig`에서 동일한 UID와 GID를 언급해야 합니다.

```
{
```

```
    "KernelGatewayImageConfig": {
        "FileSystemConfig": {
            "DefaultUid": 1000,
            "DefaultGid": 100
        }
    }
}
```

사용자 지정 이미지에 허용되는 UID/GID 값은 Studio 이미지의 경우 0/0 및 1000/100입니다. 사용자 지정 이미지 작성 및 관련된 `AppImageConfig` 설정의 예는 이 Github 리포지토리를 참조하세요.

사용자가 이를 조작하지 않도록 하려면 SageMaker Studio 노트북 사용자에게 `CreateAppImageConfigUpdateAppImageConfig`, 또는 `DeleteAppImageConfig` 권한을 부여하지 마세요.

네트워크 관리

SageMaker Studio 도메인을 설정하려면 VPC 네트워크, 서브넷, 보안 그룹을 지정해야 합니다. VPC와 서브넷을 지정할 때는 다음 섹션에서 설명하는 사용량 및 예상 증가량을 고려하여 IP를 할당해야 합니다.

VPC 네트워크 계획

SageMaker Studio 도메인과 연결된 고객 VPC 서브넷은 다음 요인에 따라 적절한 CIDR (클래스 없는 도메인 간 라우팅) 범위로 생성해야 합니다.

- 사용자 수.
- 사용자당 앱 수.
- 사용자당 고유 인스턴스 유형 수.
- 사용자당 평균 훈련 인스턴스 수.
- 예상 성장률.

SageMaker 및 참여 AWS 서비스는 다음과 같은 사용 사례를 위해 고객 VPC 서브넷에 ENI (엘라스틱 네트워크 인터페이스) 를 주입합니다.

- Amazon EFS는 도메인의 EFS 탑재 대상에 ENI를 삽입합니다 (SageMaker 도메인에 연결된 서브넷/가용 영역당 IP 하나). SageMaker
- SageMaker Studio는 사용자 프로필 또는 공유 공간에서 사용하는 모든 고유 인스턴스에 대해 ENI를 삽입합니다. 다음과 같은 예가 있습니다.
  - 사용자 프로필이 기본 Jupyter 서버 앱('시스템' 인스턴스 1개), 데이터 과학 앱 및 기본 Python 앱 (둘 다 `ml.t3.medium` 인스턴스에서 실행)을 실행하는 경우에 Studio는 두 개의 IP 주소를 주입합니다.
  - 사용자 프로필이 기본 Jupyter 서버 앱('시스템' 인스턴스 1개), Tensorflow GPU 앱 (`ml.g4dn.xlarge` 인스턴스에서), Data Wrangler 앱(`ml.m5.4xlarge` 인스턴스에서)을 실행하는 경우 Studio는 세 개의 IP 주소를 주입합니다.
- 도메인 VPC 서브넷/가용 영역의 각 VPC 엔드포인트에 대한 ENI가 삽입됩니다 (VPC 엔드포인트의 경우 4개, S3, ECR 등과 같은 참여 서비스 SageMaker VPC 엔드포인트의 경우 최대 6개). CloudWatch
- 동일한 VPC 구성으로 SageMaker 교육 및 처리 작업을 시작하는 경우 각 작업에는 인스턴스당 두 개의 IP 주소가 필요합니다.

> **Note**
>
> 서브넷 및 VPC 전용 트래픽과 같은 SageMaker Studio의 VPC 설정은 Studio에서 생성한 교육/처리 작업에 자동으로 전달되지 않습니다. SageMaker 사용자는 Create*Job API를 호출할 때 필요에 따라 VPC 설정과 네트워크 격리를 설정해야 합니다. 자세한 내용은 인터넷이 연결되지 않은 모드에서 훈련 및 추론 컨테이너 실행을 참조하세요.

시나리오: 데이터 과학자들이 서로 다른 두 가지 인스턴스 유형에 대해 실험을 실행

이 시나리오에서는 SageMaker 도메인이 VPC 전용 트래픽 모드로 설정되어 있다고 가정합니다. SageMakerAPI, SageMaker 런타임, Amazon S3 및 Amazon ECR과 같은 VPC 엔드포인트가 설정되어 있습니다.

한 데이터 과학자가 서로 다른 두 가지 인스턴스 유형(예: `ml.t3.medium` 및`ml.m5.large`)에서 실행 중인 Studio 노트북으로 각 인스턴스 유형에서 두 개의 앱을 실행하는 실험을 진행하고 있습니다.

데이터 과학자가 `ml.m5.4xlarge` 인스턴스에서 동일한 VPC 구성으로 훈련 작업을 동시에 실행한다고 가정해 보겠습니다.

이 시나리오의 경우 SageMaker 스튜디오 서비스는 다음과 같이 ENI를 주입합니다.

표 1 — 실험 시나리오를 위해 고객 VPC에 주입된 ENI

개체	대상	ENI 주입	참고	수준
EFS 탑재 대상	VPC 서브넷	3개	세 개의 AZ/서브넷	도메인
VPC 엔드포인트	VPC 서브넷	30	각각 VPCE가 10개인 AZ/서브넷 3개	도메인
Jupyter 서버	VPC 서브넷	1개	인스턴스당 IP 1개	User
KernelGateway 앱	VPC 서브넷	2개	인스턴스 유형당 IP 1개	User

개체	대상	ENI 주입	참고	수준
학습	VPC 서브넷	2개	훈련 인스턴스당 IP 2개 EFA를 사용하는 경우 훈련 인스턴스당 IP 5개	User

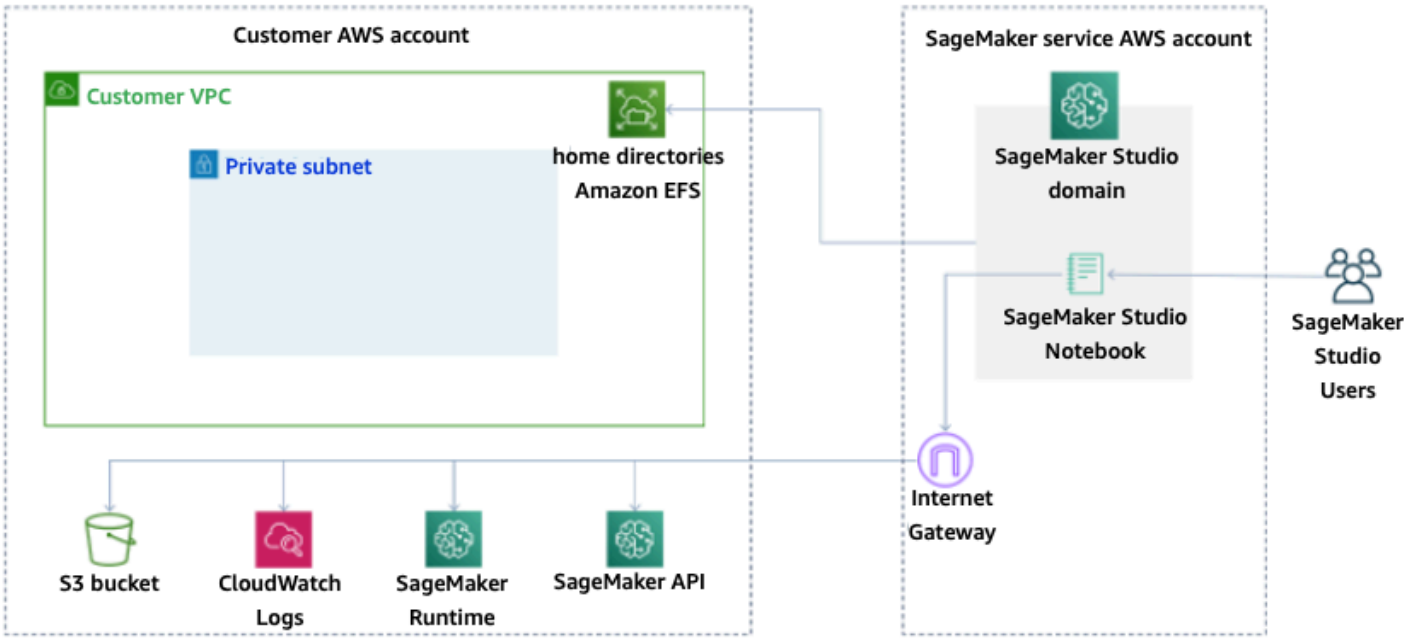
이 시나리오의 경우 고객 VPC에서 총 38개의 IP가 사용되며, 도메인 수준에서는 33개의 IP가 사용자 간에 공유되고 사용자 수준에서 5개의 IP가 사용됩니다. 이 도메인에서 유사한 사용자 프로필을 가진 100명의 사용자가 이러한 활동을 동시에 수행하는 경우 도메인 수준 IP 사용량 (서브넷당 11IP, 총 511개 IP) 외에 사용자 수준에서 5 x 100 = 500 IP를 사용하게 됩니다. 이 시나리오에서는 /22를 사용하여 1024개의 IP 주소를 할당하고 확장할 수 있는 VPC 서브넷 CIDR을 생성해야 합니다.

VPC 네트워크 옵션

SageMaker Studio 도메인은 다음 옵션 중 하나를 사용하여 VPC 네트워크를 구성할 수 있도록 지원합니다.

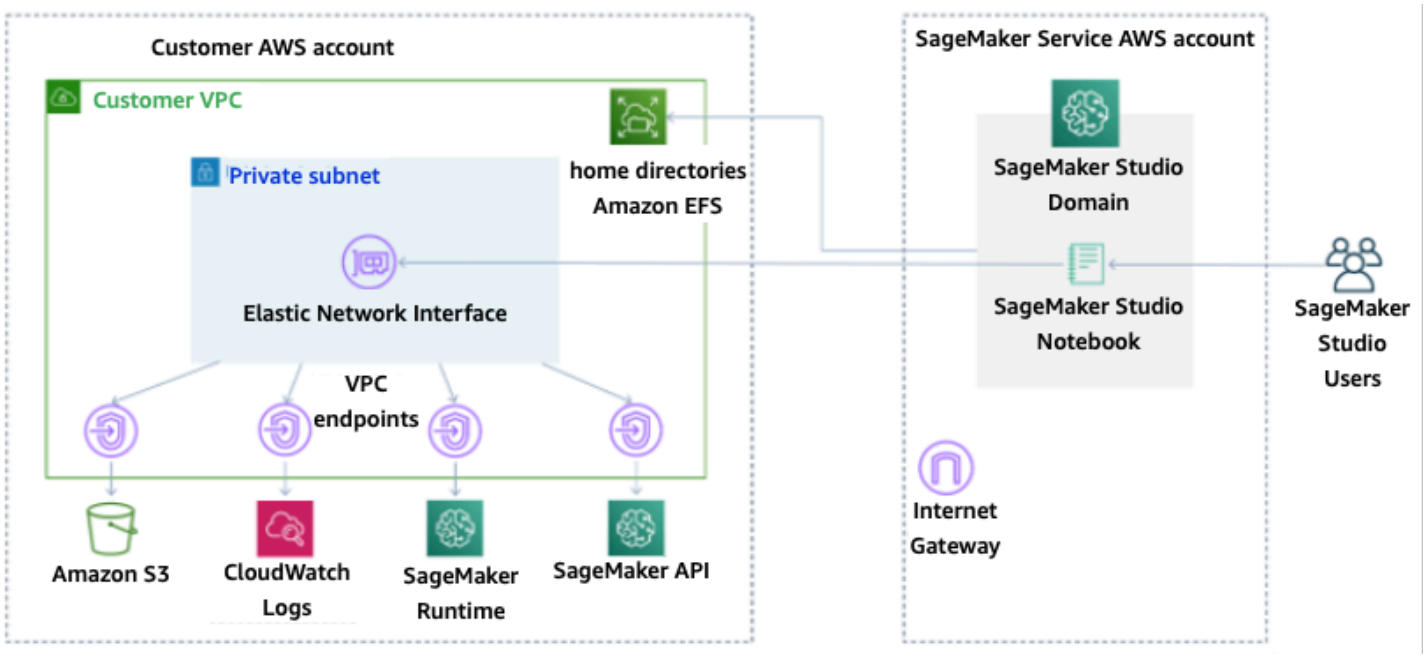
- 퍼블릭 인터넷 전용
- VPC 전용

퍼블릭 인터넷 전용 옵션을 사용하면 SageMaker API 서비스가 VPC에서 프로비저닝되고 SageMaker 서비스 계정으로 관리되는 인터넷 게이트웨이를 통해 퍼블릭 인터넷을 사용할 수 있습니다 (다음 다이어그램 참조).



기본 모드: SageMaker 서비스 계정을 통한 인터넷 액세스

VPC 전용 옵션은 다음 다이어그램에서 볼 수 있듯이 SageMaker 서비스 계정으로 관리되는 VPC로부터의 인터넷 라우팅을 비활성화하고 고객이 VPC 엔드포인트를 통해 트래픽이 라우팅되도록 구성할 수 있도록 합니다.



VPC 전용 모드: 서비스 계정을 통한 SageMaker 인터넷 액세스 불가

VPC 전용 모드로 설정된 도메인의 경우 사용자 프로필별로 보안 그룹을 설정하여 기본 인스턴스가 완전히 격리되도록 하세요. AWS 계정의 각 도메인은 고유한 VPC 구성 및 인터넷 모드를 가질 수 있습니다. VPC 네트워크 구성 설정에 대한 자세한 내용은 VPC의 Connect SageMaker Studio Notebook을 외부 리소스에 연결을 참조하십시오.

제한 사항

- SageMaker Studio 도메인을 생성한 후에는 새 서브넷을 도메인에 연결할 수 없습니다.
- VPC 네트워크 유형(퍼블릭 인터넷 전용 또는 VPC 전용)은 변경할 수 없습니다.

데이터 보호

ML 워크로드를 설계하기 전에, 보안에 영향을 미치는 기본적인 방법들을 준비해야 합니다. 예를 들어, 데이터 분류는 민감도 수준에 따라 데이터를 분류하는 방법을 제공하며, 암호화는 무단 액세스를 할 경우 데이터를 이해할 수 없게 만들어 데이터를 보호합니다. 이러한 방법이 중요한 이유는, 조작 부주의 방지 또는 규제 의무 사항 준수와 같은 목표의 달성을 지원하기 때문입니다.

SageMaker Studio는 저장 데이터와 전송 중 데이터를 보호하기 위한 여러 기능을 제공합니다. 하지만 AWS공동 책임 모델에 설명된 바와 같이, 고객은 AWS 글로벌 인프라에서 호스팅되는 콘텐츠에 대한 통제권을 유지할 책임이 있습니다. 이 섹션에서는 고객이 이러한 기능을 사용하여 데이터를 보호하는 방법에 대해 설명합니다.

저장 데이터 보호

SageMaker는 모델 구축 데이터 및 모델 아티팩트와 함께 SageMaker Studio 노트북을 보호하기 위해 노트북은 물론 훈련 및 일괄 변환 작업의 결과물도 암호화합니다. SageMaker는 기본적으로 Amazon S3용 AWS 관리형 키를 사용하여 이를 암호화합니다. 이 Amazon S3용 AWS 관리형 키는 크로스 계정 액세스를 위해 공유할 수 없습니다. 크로스 계정 액세스의 경우 SageMaker 리소스를 생성할 때 고객 관리형 키를 지정하여 크로스 계정 액세스를 위해 공유할 수 있도록 하세요.

SageMaker Studio를 사용하면 다음 위치에 데이터를 저장할 수 있습니다.

- S3 버킷 — 공유 가능한 노트북이 활성화되면, SageMaker Studio는 노트북 스냅샷과 메타데이터를 S3 버킷에 공유합니다.
- EFS 볼륨 - SageMaker Studio는 노트북과 데이터 파일을 저장하기 위해 EFS 볼륨을 도메인에 연결합니다. 이 EFS 볼륨은 도메인이 삭제된 후에도 유지됩니다.
- EBS 볼륨 — EBS는 노트북이 실행되는 인스턴스에 연결됩니다. 이 볼륨은 인스턴스 기간 동안 지속됩니다.

AWS KMS를 사용한 유휴 시 암호화

- AWS KMS 키를 전달하여 노트북, 훈련, 튜닝, 일괄 변환 작업 및 엔드포인트에 연결된 EBS 볼륨을 암호화할 수 있습니다.
- KMS 키를 지정하지 않는 경우 SageMaker는 시스템 관리형 KMS 키를 사용하여 운영 체제(OS) 볼륨과 ML 데이터 볼륨을 모두 암호화합니다.

- 규정 준수를 위해 KMS 키로 암호화해야 하는 민감한 데이터는 ML 스토리지 볼륨 또는 Amazon S3에 저장해야 합니다. 두 가지 모두 지정한 KMS 키를 사용하여 암호화할 수 있습니다.

전송 중 데이터 보호

SageMaker Studio는 ML 모델 아티팩트 및 기타 시스템 아티팩트가 전송 중이거나 저장된 상태일 때 암호화되도록 합니다. SageMaker API 및 콘솔에 대한 요청은 안전한 SSL 연결을 통해 전달됩니다. 일부 인트라 네트워크의 전송 중 데이터(서비스 플랫폼 내)는 암호화되지 않습니다. 여기에는 다음이 포함됩니다.

- 서비스 컨트롤 플레인과 훈련 작업 인스턴스(고객 데이터 아님) 간의 명령 및 제어 통신.
- 분산 처리 및 훈련 작업(인트라 네크워크)의 노드 간 통신.

하지만 훈련 클러스터의 노드 간 통신을 암호화하도록 선택할 수도 있습니다. 컨테이너 간 트래픽 암호화를 활성화하면 훈련 시간이 늘어날 수 있는데, 분산된 딥 러닝 알고리즘을 사용하는 경우 특히 더 그렇습니다.

기본적으로 Amazon SageMaker는 데이터를 안전하게 보호하기 위해 Amazon VPC에서 훈련 작업을 실행합니다. 프라이빗 VPC를 구성하여 훈련 컨테이너 및 데이터를 보호하기 위한 보안 수준을 하나 더 추가할 수 있습니다. 또한 SageMaker Studio 도메인이 VPC 전용 모드에서 실행되도록 구성하고, 인터넷을 통해 트래픽을 유출하지 않고 사설 네트워크를 통해 트래픽을 라우팅하도록 VPC 엔드포인트를 설정할 수 있습니다.

데이터 보호 가드레일

저장 중인 SageMaker 호스팅 볼륨 암호화

온라인 추론을 위해 SageMaker 엔드포인트를 호스팅하는 동안 암호화를 적용하려면 다음 정책을 사용하세요.

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Encryption",
         "Effect": "Allow",
         "Action": [
```

```
            "sagemaker:CreateEndpointConfig"
        ],
        "Resource": "*",
        "Condition": {
            "Null": {
                "sagemaker:VolumeKmsKey": "false"
            }
        }
    }
  ]
}
```

모델 모니터링 중에 사용되는 S3 버킷 암호화하기

모델 모니터링은 SageMaker 엔드포인트로 전송된 데이터를 캡처하여 S3 버킷에 저장합니다. 데이터 캡처 구성을 설정할 때, S3 버킷을 암호화해야 합니다. 현재 이에 대한 보완 제어 기능은 없습니다.

모델 모니터링 서비스는 엔드포인트 출력을 캡처하는 것 외에도, 사전 지정된 기준선을 기준으로 드리프트를 확인합니다. 드리프트를 모니터링하는 데 사용되는 출력 및 중간 스토리지 볼륨을 암호화해야 합니다.

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Encryption",
         "Effect": "Allow",
         "Action": [
             "sagemaker:CreateMonitoringSchedule",
             "sagemaker:UpdateMonitoringSchedule"
         ],
         "Resource": "*",
         "Condition": {
             "Null": {
                 "sagemaker:VolumeKmsKey": "false",
                 "sagemaker:OutputKmsKey": "false"
             }
         }
     }
   ]
}
```

SageMaker Studio 도메인 스토리지 볼륨 암호화

Studio 도메인에 연결된 스토리지 볼륨에 암호화를 적용합니다. 이 정책은 사용자가 스튜디오 도메인에 연결된 스토리지 볼륨을 암호화하기 위해 CMK를 제공하도록 요구합니다.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "EncryptDomainStorage",
             "Effect": "Allow",
             "Action": [
                 "sagemaker:CreateDomain"
             ],
             "Resource": "*",
             "Condition": {
                 "Null": {
                     "sagemaker:VolumeKmsKey": "false"
                 }
             }
         }
     ]
 }
```

노트북을 공유하는 데 사용되는 S3에 저장된 데이터를 암호화합니다.

다음은 SageMaker Studio 도메인의 사용자 간에 노트북을 공유하는 데 사용되는 버킷에 저장된 모든 데이터를 암호화하는 정책입니다.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "EncryptDomainSharingS3Bucket",
             "Effect": "Allow",
             "Action": [
                 "sagemaker:CreateDomain",
                 "sagemaker:UpdateDomain"
             ],
             "Resource": "*",
             "Condition": {
                 "Null": {
```

```
                    "sagemaker:DomainSharingOutputKmsKey": "false"
                }
            }
        }
    ]
}
```

제한 사항

- 도메인이 생성되면, 연결된 EFS 볼륨 스토리지를 사용자 지정 AWS KMS 키로 업데이트할 수 없습니다.
- 훈련/처리 작업 또는 엔드포인트 구성을 생성한 후에는, KMS 키를 사용하여 업데이트할 수 없습니다.

로깅 및 모니터링

컴파일 작업, 처리 작업, 훈련 작업, 엔드포인트, 변환 작업, 노트북 인스턴스 및 노트북 인스턴스 수명 주기 구성을 디버그하는 데 도움이 되도록 알고리즘 컨테이너, 모델 컨테이너 또는 노트북 인스턴스 수명 주기 구성이 stdout 또는 stderr로 전송되며 Amazon CloudWatch Logs로도 전송됩니다. 원시 데이터를 수집하여 처리해서, 읽기 가능하며 실시간에 가까운 지표로 변환하는 Amazon CloudWatch를 통해 SageMaker Studio를 모니터링할 수 있습니다. 이러한 통계는 15개월 동안 보관되므로, 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다.

CloudWatch를 사용한 로깅

데이터 과학 프로세스는 기본적으로 실험적이고 반복적이므로 노트북 사용, 훈련/처리 작업 실행 시간, 훈련 지표, 간접 호출 대기 시간과 같은 엔드포인트 서비스 지표와 같은 활동을 기록하는 것이 필수적입니다. 기본적으로 SageMaker는 지표를 CloudWatch Logs에 게시하며 이러한 로그는 AWS KMS를 사용하여 고객 관리형 키로 암호화할 수 있습니다.

또한 공용 인터넷을 사용하지 않고도 VPC 엔드포인트를 사용하여 CloudWatch에 로그를 보낼 수 있습니다. 특정 임계값을 주시하다가 해당 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 정보는 Amazon CloudWatch 사용 설명서를 참조하세요.

SageMaker는 `/aws/sagemaker/studio` 아래에 한 개의 스튜디오용 로그 그룹을 생성합니다. 각 사용자 프로필 및 앱은 이 로그 그룹 아래에 고유한 로그 스트림을 가지며 생명 주기 구성 스크립트에도 자체 로그 스트림이 있습니다. 예를 들어 Jupyter 서버 앱이 있고 수명 주기 스크립트가 첨부된 'studio-user'라는 사용자 프로필과 데이터 과학 커널 게이트웨이 앱의 로그 스트림은 다음과 같습니다.

`/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default`

`/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default/LifecycleConfigOnStart`

`/aws/sagemaker/studio/<domain-id>/studio-user/KernelGateway/datascience-app`

SageMaker가 사용자를 대신하여 CloudWatch에 로그를 전송하려면 훈련/처리/변환 작업 API의 호출자에게 다음 권한이 필요합니다.

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

```
        {
            "Action": [
                "logs:CreateLogDelivery",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DeleteLogDelivery",
                "logs:Describe*",
                "logs:GetLogEvents",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries",
                "logs:PutLogEvents",
                "logs:PutResourcePolicy",
                "logs:UpdateLogDelivery"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

사용자 지정 AWS KMS 키로 이러한 로그를 암호화하려면 먼저 CloudWatch 서비스가 키를 암호화하고 해독할 수 있도록 키 정책을 수정해야 합니다. 로그 암호화 AWS KMS 키를 생성한 후에는 다음을 포함하도록 키 정책을 수정하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
```

```
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:region:account-
id:*"
                }
            }
        }
    ]
}
```

언제든지 ArnEquals을 사용하여 암호화하려는 CloudWatch 로그에 대해 특정 Amazon 리소스 이름(ARN) 을 제공할 수 있습니다. 여기서는 간소화를 위해 이 키를 사용하여 계정의 모든 로그를 암호화할 수 있음을 보여줍니다. 또한 훈련, 처리 및 모델 엔드포인트는 인스턴스 CPU 및 메모리 사용률, 호스팅 간접 호출 지연 시간 등에 대한 지표를 게시합니다. 또한 특정 임계값을 초과할 경우 관리자에게 이벤트를 알리도록 Amazon SNS를 구성할 수 있습니다. 훈련 및 처리 API의 소비자는 다음과 같은 권한을 가져야 합니다.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "cloudwatch:DeleteAlarms",
                 "cloudwatch:DescribeAlarms",
                 "cloudwatch:GetMetricData",
                 "cloudwatch:GetMetricStatistics",
                 "cloudwatch:ListMetrics",
                 "cloudwatch:PutMetricAlarm",
                 "cloudwatch:PutMetricData",
                 "sns:ListTopics"
             ],
             "Resource": "*",
             "Effect": "Allow",
             "Condition": {
                 "StringLike": {
                     "cloudwatch:namespace": "aws/sagemaker/*"
                 }
             }

         },
         {
             "Action": [
                 "sns:Subscribe",
                 "sns:CreateTopic"
```

```
            ],
            "Resource": [
                "arn:aws:sns:*:*:*SageMaker*",
                "arn:aws:sns:*:*:*Sagemaker*",
                "arn:aws:sns:*:*:*sagemaker*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AWS CloudTrail을 통한 감사

규정 준수 태세를 개선하려면 AWS CloudTrail을 사용하여 모든 API를 감사하십시오. 기본적으로 모든 SageMaker API는 AWS CloudTrail로 로깅됩니다. CloudTrail을 사용하기 위해 IAM 권한이 추가로 필요하지 않습니다.

`InvokeEndpoint` 및 `InvokeEndpointAsync`를 제외한 모든 SageMaker 작업은 CloudTrail에 의해 로깅되고 해당 작업에 기록됩니다. 예를 들어 `CreateTrainingJob`, `CreateEndpoint` 및 `CreateNotebookInstance` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 CloudTrail 이벤트 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS IAM 사용자 보안 인증 정보로 했는지 여부.
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부. 예제 이벤트를 보려면 CloudTrail을 사용한 로그 SageMaker API 호출 설명서를 참조하세요.

기본적으로 CloudTrail은 사용자 프로필의 Studio 실행 역할 이름을 각 이벤트의 식별자로 로깅합니다. 이는 각 사용자에게 고유한 실행 역할이 있는 경우 작동합니다. 여러 사용자가 동일한 실행 역할을 공유하는 경우, `sourceIdentity` 구성을 사용하여 Studio 사용자 프로필 이름을 CloudTrail에 전파할 수 있습니다. `sourceIdentity` 기능을 활성화하려면 Amazon SageMaker Studio에서 사용자 리소스 액세스 모니터링을 참조하세요. 공유 스페이스에서는 모든 작업이 스페이스 ARN을 소스로 참조하므로 `sourceIdentity`를 통해 감사할 수 없습니다.

비용 분담

SageMaker Studio에는 관리자가 개별 도메인, 공유 스페이스 및 사용자의 지출을 추적하는 데 도움이 되는 기능이 내장되어 있습니다.

자동 태그 지정

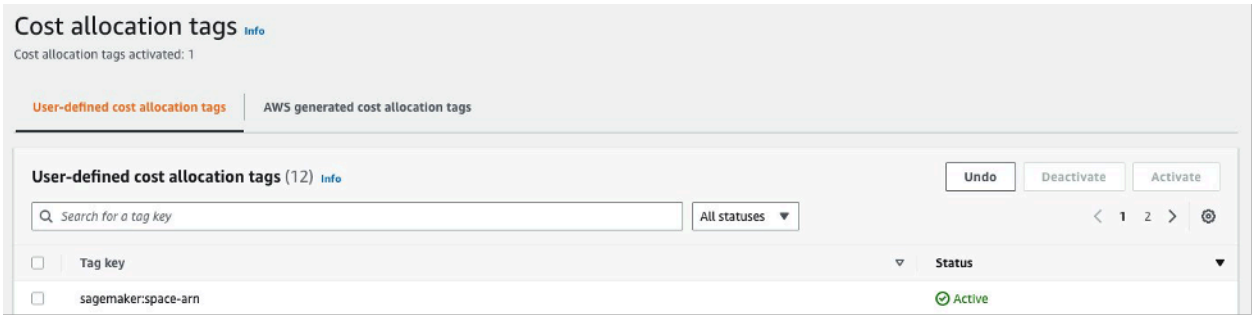
이제 SageMaker Studio는 훈련 작업, 처리 작업, 커널 앱과 같은 새로운 SageMaker 리소스에 개별 `sagemaker:domain-arn`을 사용하여 자동으로 태그를 지정합니다. 또한 SageMaker는 보다 세분화된 수준에서 리소스에 `sagemaker:user-profile-arn` 또는 `sagemaker:space-arn`의 태그를 지정하여 리소스의 주요 작성자를 지정합니다.

SageMaker 도메인 EFS 볼륨에는 도메인 ARN 값과 함께 `ManagedByAmazonSageMakerResource`라는 이름의 키가 태그 지정됩니다. 여기에는 사용자 레벨별 스페이스 사용량을 파악할 수 있는 세분화된 태그가 없습니다. 하지만 관리자는 EFS 볼륨을 EC2 인스턴스에 연결하여 맞춤형 모니터링을 할 수 있습니다.

비용 모니터링

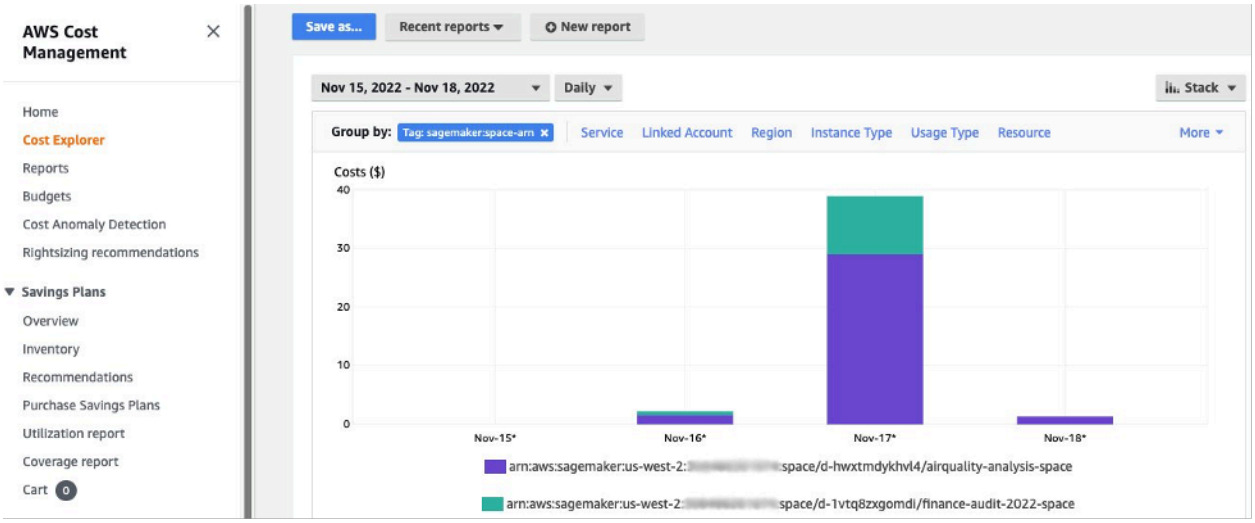
자동 태그를 사용하면 관리자는 AWS 비용 및 사용 보고서(CUR)의 데이터를 기반으로 구축된 사용자 지정 솔루션뿐만 아니라 AWS Cost Explorer 및 AWS Budgets 등의 특별한 솔루션을 통해 ML 지출을 추적, 보고 및 모니터링할 수 있습니다.

첨부된 태그를 비용 분석에 사용하려면 먼저 AWS Billing 콘솔의 비용 할당 태그 섹션에서 태그를 활성화해야 합니다. 태그가 비용 할당 태그 패널에 표시되는 데 최대 24시간이 걸릴 수 있으므로. 활성화하기 전에 SageMaker 리소스를 생성해야 합니다.



Cost Explorer에서 비용 할당 태그로 활성화된 스페이스 ARN

비용 할당 태그를 활성화하면 AWS가 태그가 지정된 리소스를 추적하기 시작하며, 24~48시간 후에 Cost Explorer에서 태그가 선택 가능한 필터로 표시됩니다.



샘플 도메인의 공유 스페이스별로 그룹화된 비용

비용 관리

첫 번째 SageMaker Studio 사용자가 온보딩되면, SageMaker는 도메인용 EFS 볼륨을 생성합니다. 노트북과 데이터 파일이 사용자의 홈 디렉터리에 저장되므로, 이 EFS 볼륨의 경우 스토리지 비용이 발생합니다. 사용자가 Studio 노트북을 시작하면, Studio 노트북은 노트북을 실행하는 컴퓨팅 인스턴스용으로 시작됩니다. 자세한 비용 내역은 Amazon SageMaker 요금을 참조하십시오.

관리자는 일반 가드레일 섹션에 언급된 대로 IAM 정책을 사용하여 사용자가 실행할 수 있는 인스턴스 목록을 지정하여 컴퓨팅 비용을 제어할 수 있습니다. 또한 유휴 상태인 앱을 자동으로 종료하여 비용을 절감하려면 SageMaker Studio 자동 종료 확장을 사용하는 것이 좋습니다. 이 서버 확장 프로그램은 사용자 프로필별로 실행 중인 앱을 정기적으로 폴링하고 관리자가 설정한 제한 시간에 따라 유휴 앱을 종료합니다.

도메인의 모든 사용자에 대해 이 확장을 설정하려면 사용자 지정 섹션에 설명된 대로 수명 주기 구성을 사용할 수 있습니다. 또한 확장 검사기를 사용하여 모든 도메인 사용자에게 확장이 설치되어 있는지 확인할 수도 있습니다.

사용자 지정

수명 주기 구성

수명 주기 구성은 SageMaker Studio 수명 주기 이벤트(예: 새 SageMaker Studio 노트북 시작)에 의해 시작되는 쉘 스크립트입니다. 이러한 쉘 스크립트를 사용하여 사용자 정의 패키지 설치, 비활성 노트북 앱 자동 종료를 위한 Jupyter 확장, Git 구성 설정과 같은 SageMaker Studio 환경의 사용자 지정을 자동화할 수 있습니다. 수명 주기 구성을 구축하는 방법에 대한 자세한 지침은 수명 주기 구성을 사용한 Amazon SageMaker Studio 사용자 지정 블로그를 참조하세요.

SageMaker Studio 노트북용 사용자 지정 이미지

Strudio 노트북은 사전 빌드된 이미지 세트와 함께 제공됩니다. 이 이미지 세트는 Amazon SageMaker Python SDK 및 최신 버전의 IPython 런타임 또는 커널로 구성되어 있습니다. 이 기능을 사용하면 Amazon SageMaker 노트북으로 사용자 지정 이미지를 가져올 수 있습니다. 이렇게 하면 도메인에서 인증된 모든 사용자가 해당 이미지를 사용할 수 있습니다.

개발자와 데이터 과학자는 아래의 다양한 사용 사례에 맞는 사용자 지정 이미지를 요구할 수 있습니다.

- TensorFlow, MXNet, PyTorch 등과 같은 인기 있는 ML 프레임워크의 특정 또는 최신 버전에 대한 액세스.
- 신속한 반복 및 모델 훈련 수행을 위하여 로컬에서 개발한 사용자 지정 코드 또는 알고리즘을 SageMaker Studio 노트북으로 가져오기.
- API를 통해 데이터 레이크 또는 온프레미스 데이터 스토어에 액세스. 관리자는 이미지에 해당 드라이버를 포함해야 합니다.
- IPython 이외(예: R, Julia 및 기타)의 백엔드 런타임(커널이라고도 함)에 대한 액세스. 설명된 방법을 사용하여 사용자 지정 커널을 설치할 수도 있습니다.

사용자 지정 이미지를 만드는 방법에 대한 자세한 지침은 사용자 지정 SageMaker 이미지 만들기를 참조하세요.

JupyterLab 확장

SageMaker Studio JuypterLab 3 노트북을 사용하면 계속 성장하고 있는 오픈 소스 JupyterLab 확장 커뮤니티를 활용할 수 있습니다. 이 섹션에서는 SageMaker 개발자 워크플로에 자연스럽게 맞는 몇 가지를 중점적으로 설명하지만 사용 가능한 확장을 찾아보거나 직접 만드는 것이 좋습니다.

이제 JupyterLab 3를 사용하면 확장을 패키징하고 설치하는 프로세스가 훨씬 쉬워집니다. bash 스크립트를 통해 앞서 언급한 확장을 설치할 수 있습니다. 예를 들어, SageMaker Studio에서 Studio 런처에서 시스템 터미널을 열고 다음 명령을 실행해 볼 수 있습니다. 또한 수명 주기 구성을 사용하여 이러한 확장의 설치를 자동화하여 Studio를 다시 시작해도 유지되도록 할 수 있습니다. 도메인의 모든 사용자에 대해, 또는 개별 사용자 수준에서 이를 구성할 수 있습니다.

예를 들어 Amazon S3 파일 브라우저용 확장을 설치하려면 시스템 터미널에서 다음 명령을 실행하고 브라우저를 새로 고쳐야 합니다.

```
conda init
conda activate studio
pip install jupyterlab_s3_browser
jupyter serverextension enable --py jupyterlab_s3_browser
conda deactivate
restart-jupyter-server
```

확장 관리에 대한 자세한 내용은 JupyterLab 및 Jupyter 서버 확장 설치를 참조하세요. 여기에는 이전 버전과의 호환성을 위해 JupyterLab 노트북 버전 1과 3에서 모두 작동하는 수명 주기 구성을 작성하는 방법도 포함되어 있습니다.

Git 리포지토리

SageMaker Studio에는 사용자가 Git 리포지토리의 맞춤형 URL을 입력하고, EFS 디렉터리에 복제하고, 변경 사항을 푸시하고, 커밋 이력을 볼 수 있도록 Jupyter Git 확장이 사전 설치되어 있습니다. 관리자는 도메인 수준에서 제안된 Git 리포지토리를 구성하여 최종 사용자에게 드롭다운 선택 항목으로 표시되도록 할 수 있습니다. Studio에 제안된 Git 리포지토리 첨부에서 최신 지침을 참조하세요.

리포지토리가 비공개인 경우, 이 확장은 표준 Git 설치를 사용하여 터미널에 보안 인증 정보를 입력하도록 사용자에게 요청합니다. 아니면 사용자가 개별 EFS 디렉터리에 ssh 보안 인증 정보를 저장하여 보다 쉽게 관리할 수도 있습니다.

Conda 환경

SageMaker Studio 노트북은 Amazon EFS를 영구 스토리지 계층으로 사용합니다. 데이터 과학자는 영구 스토리지를 사용하여 사용자 지정 conda 환경을 만들고 이러한 환경을 사용하여 커널을 생성할 수 있습니다. 이러한 커널은 EFS에서 지원되며 커널, 앱 또는 Studio를 다시 시작해도 지속됩니다. Studio는 모든 유효한 환경을 KernelGateway 커널로 자동 선택합니다.

conda 환경을 만드는 과정은 데이터 과학자에게 간단한 일이지만, 커널이 커널 선택기에 채워지는 데는 약 1분이 걸립니다. 환경을 만들려면 시스템 터미널에서 다음을 실행하세요.

```
mkdir -p ~/.conda/envs
conda create --yes -p ~/.conda/envs/custom
conda activate ~/.conda/envs/custom
conda install -y ipykernel
conda config --add envs_dirs ~/.conda/envs
```

Amazon SageMaker Studio 노트북에서 Python 패키지를 관리하는 네 가지 접근 방식에서 스튜디오 EFS 볼륨에서의 Persist Conda 환경 섹션을 참조하세요.

결론

이 백서에서는 플랫폼 관리자가 SageMaker Studio 플랫폼을 설정하고 관리할 수 있게 하는 운영 모델, 도메인 관리, 자격 증명 관리, 권한 관리, 네트워크 관리, 로깅, 모니터링 및 사용자 지정 등에 대한 몇 가지 모범 사례를 검토합니다.

부록

멀티테넌시 비교

표 2 — 멀티테넌시 비교

멀티 도메인	다중 계정	단일 도메인 내 속성 기반 액세스 제어 (ABAC)
태그를 사용하여 리소스를 격리할 수 있습니다. SageMaker Studio는 도메인 ARN 및 사용자 프로필/스페이스 ARN으로 모든 리소스에 자동으로 태그를 지정합니다.	각 테넌트는 자체 계정에 속하므로 리소스가 완전히 격리됩니다.	리소스 격리는 태그를 사용하여 이루어집니다. 사용자는 ABAC에 대해 생성된 리소스의 태그 지정을 관리해야 합니다.
목록 API는 태그로 제한할 수 없습니다. 리소스의 UI 필터링은 공유 공간에서 수행되지만 AWS CLI 또는 Boto3 SDK를 통해 이루어진 List API 호출은 지역 전체의 리소스를 나열합니다.	테넌트가 전용 계정을 사용하기 때문에 List API 격리도 가능합니다.	목록 API는 태그로 제한할 수 없습니다. AWS CLI 또는 Boto3 SDK를 통해 이루어진 목록 API 호출은 지역 전체의 리소스를 나열합니다.
SageMaker Domain ARN을 비용 할당 태그로 사용하여 테넌트당 스튜디오 컴퓨팅 및 스토리지 비용을 쉽게 모니터링할 수 있습니다.	SageMaker 테넌트별 Studio 컴퓨팅 및 스토리지 비용은 전용 계정을 사용하여 쉽게 모니터링할 수 있습니다.	SageMaker 테넌트당 스튜디오 컴퓨팅 비용은 사용자 지정 태그를 사용하여 계산해야 합니다. SageMaker 모든 테넌트가 동일한 EFS 볼륨을 공유하므로 도메인별로 스튜디오 스토리지 비용을 모니터링할 수 없습니다.

멀티 도메인	다중 계정	단일 도메인 내 속성 기반 액세스 제어 (ABAC)
서비스 할당량은 계정 수준에서 설정되므로 단일 테넌트가 여전히 모든 리소스를 사용할 수 있습니다.	서비스 할당량은 각 테넌트의 계정 수준에서 설정할 수 있습니다.	서비스 할당량은 계정 수준에서 설정되므로 단일 테넌트가 여전히 모든 리소스를 사용할 수 있습니다.
코드형 인프라 (IaC) 또는 Service Catalog를 통해 여러 테넌트로 확장할 수 있습니다.	여러 테넌트로 확장하려면 Organizations와 여러 계정을 판매해야 합니다.	규모를 조정하려면 각 새 테넌트에 대한 테넌트별 역할이 필요하며 사용자 프로필에는 테넌트 이름으로 수동으로 태그를 지정해야 합니다.
공유 공간을 통해 테넌트 내 사용자 간의 협업이 가능합니다.	공유 공간을 통해 테넌트 내 사용자 간 협업이 가능합니다.	모든 테넌트는 협업을 위해 동일한 공유 공간에 액세스할 수 있습니다.

SageMaker Studio 도메인 백업 및 복구

실수로 EFS를 삭제하거나 네트워킹 또는 인증 변경으로 인해 도메인을 다시 생성해야 하는 경우 다음 지침을 따르세요.

옵션 1: EC2를 사용하여 기존 EFS에서 백업

SageMaker 스튜디오 도메인 백업

1. SageMaker 스튜디오 (CLI, SDK) 의 사용자 프로필 및 스페이스를 나열합니다.
2. 사용자 프로필/스페이스를 EFS의 UID에 매핑합니다.
   a. 사용자/스페이스 목록의 각 사용자에 대해 사용자 프로필/스페이스(CLI, SDK)를 설명합니다.
   b. 사용자 프로필/스페이스를 `HomeEfsFileSystemUid`에 매핑합니다.
   c. 사용자에게 고유한 실행 역할이 있다면 `UserSettings['ExecutionRole']`에 사용자 프로필을 매핑합니다.
   d. 기본 스페이스 실행 역할을 식별합니다.
3. 새 도메인을 만들고 기본 스페이스 실행 역할을 지정합니다.
4. 사용자 프로필 및 스페이스를 생성합니다.

- 사용자 목록의 각 사용자에 대해 실행 역할 매핑을 사용하여 사용자 프로필(CLI, SDK)을 생성합니다.

5. 새 EFS와 UID에 대한 매핑을 생성합니다.
   a. 사용자 목록의 각 사용자에 대해 사용자 프로필(CLI, SDK)을 설명합니다.
   b. `HomeEfsFileSystemUid`에 사용자 프로필을 매핑합니다.
6. 필요한 경우 모든 앱, 사용자 프로필, 스페이스를 삭제한 다음 도메인을 삭제합니다.

EFS 백업

EFS를 백업하려면 다음 지침을 따르세요.

1. EC2 인스턴스를 시작하고 이전 SageMaker Studio 도메인의 인바운드/아웃바운드 보안 그룹을 새 EC2 인스턴스에 연결합니다 (포트 2049에서 TCP를 통한 NFS 트래픽 허용). VPC의 Connect SageMaker Studio 노트북을 외부 리소스에 연결을 참조하십시오.
2. SageMaker Studio EFS 볼륨을 새 EC2 인스턴스에 마운트합니다. EFS 파일 시스템 탑재를 참조하세요.
3. 파일을 EBS 로컬 스토리지로 복사합니다: `>sudo cp -rp /efs /studio-backup:`
   a. 새 도메인 보안 그룹을 EC2 인스턴스에 연결합니다.
   b. 새 EFS 볼륨을 EC2 인스턴스에 탑재합니다.
   c. 파일을 새 EFS 볼륨에 복사합니다.
   d. 사용자의 컬렉션에 있는 각 사용자에 대해:
      i. `mkdir new_uid` 디렉터리를 만듭니다.
      ii. 이전 UID 디렉터리에서 새 UID 디렉터리로 파일을 복사합니다.
      iii. 모든 파일의 소유권을 변경합니다: 모든 파일에 `chown <new_UID>`를 실행하세요.

옵션 2: S3 및 수명 주기 구성을 사용하여 기존 EFS에서 백업

1. Amazon Linux 2를 사용하는 Amazon SageMaker 노트북 인스턴스로 작업 마이그레이션을 참조하십시오.
2. 백업용 S3 버킷을 생성합니다(예:`>studio-backup`).
3. 실행 역할이 있는 모든 사용자 프로필을 나열합니다.
4. 현재 SageMaker Studio 도메인에서 도메인 수준에서 기본 LCC 스크립트를 설정합니다.

- LCC에서 /home/sagemaker-user에 있는 모든 내용을 S3의 사용자 프로필 접두사(예: s3://studio-backup/studio-user1)에 복사합니다.

5. LCC를 실행하기 위해 기본 Jupyter 서버 앱을 모두 다시 시작합니다.
6. 모든 앱, 사용자 프로필, 도메인을 삭제합니다.
7. 새 SageMaker Studio 도메인을 생성합니다.
8. 사용자 프로필 및 실행 역할 목록에서 새 사용자 프로필을 생성합니다.
9. 도메인 수준에서 LCC 설정:
   - LCC에서 S3의 사용자 프로필 접두사에 있는 모든 내용을 /home/sagemaker-user에 복사합니다.
10. LCC 구성(CLI, SDK)을 사용하여 모든 사용자를 위한 기본 Jupyter 서버 앱을 생성합니다.

SageMaker SAML 어설션을 사용한 스튜디오 액세스

솔루션 설정:

1. 외부 IdP에서 SAML 애플리케이션을 생성합니다.
2. IAM에서 외부 IdP를 ID 제공업체로 설정합니다.
3. (함수 URL 또는 API 게이트웨이를 통해) IdP가 액세스할 수 있는 SAMLValidator Lambda 함수를 생성합니다.
4. GeneratePresignedUrl Lambda 함수와 API 게이트웨이를 생성하여 함수에 액세스합니다.
5. 사용자가 API 게이트웨이를 간접적으로 호출하기 위해 수임할 수 있는 IAM 역할을 만듭니다. 이 역할은 SAML 어설션에서 다음 형식의 속성으로 전달되어야 합니다.
   - 속성 이름: https://aws.amazon.com/SAML/Attributes/Role
   - 속성 값: <IdentityProviderARN>, <RoleARN>
6. SAML 어설션 소비자 서비스(ACS) 엔드포인트를 SAMLValidator 간접 호출 URL로 업데이트합니다.

SAML 유효성 검사기 예제 코드:

```
import requests
import os
import boto3
from urllib.parse import urlparse, parse_qs
import base64
```

```
import requests
from aws_requests_auth.aws_auth import AWSRequestsAuth
import json


# Config for calling AssumeRoleWithSAML
idp_arn = "arn:aws:iam::0123456789:saml-provider/MyIdentityProvider"
api_gw_role_arn = 'arn:aws:iam:: 0123456789:role/APIGWAccessRole'
studio_api_url = "abcdef.execute-api.us-east-1.amazonaws.com"
studio_api_gw_path = "https://" + studio_api_url + "/Prod "

# Every customer will need to get SAML Response from the POST call
def get_saml_response(event):
    saml_response_uri = base64.b64decode(event['body']).decode('ascii')
    request_body = parse_qs(saml_response_uri)
    print(f"b64 saml response: {request_body['SAMLResponse'][0]}")
    return request_body['SAMLResponse'][0]


def lambda_handler(event, context):
    sts = boto3.client('sts')

    # get temporary credentials
    response = sts.assume_role_with_saml(
                    RoleArn=api_gw_role_arn,
                    PrincipalArn=durga_idp_arn,
                    SAMLAssertion=get_saml_response(event)
                )
    auth = AWSRequestsAuth(aws_access_key=response['Credentials']['AccessKeyId'],
                      aws_secret_access_key=response['Credentials']['SecretAccessKey'],
                      aws_host=studio_api_url,
                      aws_region='us-west-2',
                      aws_service='execute-api',
                      aws_token=response['Credentials']['SessionToken'])

    presigned_response = requests.post(
        studio_api_gw_path,
        data=saml_response_data,
        auth=auth)

    return presigned_response
```

참조 자료

- AWS에서 안전하며 잘 관리되는 기계 학습 환경 설정하기 (AWS 블로그)
- 완벽한 리소스 격리를 통해 팀 및 그룹을 위한 Amazon SageMaker Studio 구성하기(AWS 블로그)
- AWS SSO 및 Okta 유니버설 디렉터리를 통한 Amazon SageMaker Studio 온보딩(AWS 블로그)
- AWS 계정 페더레이션을 위한 SAML 2.0 구성 방법(Okta 설명서)
- AWS에서 안전한 엔터프라이즈 기계 학습 플랫폼 구축(AWS 기술 가이드)
- 수명 주기 구성을 사용하여 Amazon SageMaker Studio 사용자 지정하기(AWS 블로그)
- Amazon SageMaker Studio 노트북으로 사용자 지정 컨테이너 이미지 가져오기(AWS 블로그)
- 사용자 지정 SageMaker 프로젝트 템플릿 제작 — 모범 사례(AWS 블로그)
- Amazon SageMaker Pipelines를 사용한 다중 계정 모델 배포(AWS 블로그)
- 1부: NatWest Group이 확장 가능하고 안전하며 지속 가능한 MLOps 플랫폼을 구축한 방법(AWS 블로그)
- 안전한 Amazon SageMaker Studio의 미리 서명된 URL 1부: 기본 인프라(AWS 블로그)

기여자

다음은 이 문서의 기여자입니다.

- Ram Vittal, ML 솔루션스 아키텍트, Amazon Web Services
- Sean Morgan, ML 솔루션스 아키텍트, Amazon Web Services
- Durga Sury, ML 솔루션스 아키텍트, Amazon Web Services

아이디어, 수정 및 관점을 제공해 주신 다음 분들께 특별히 감사드립니다.

- Alessandro Cerè, AI/ML 솔루션스 아키텍트, Amazon Web Services
- Sumit Thakur, SageMaker 제품 리더, Amazon Web Services
- Han Zhang, 선임 소프트웨어 개발 엔지니어, Amazon Web Services
- Bhadrinath Pani, 소프트웨어 개발 엔지니어, Amazon Web Services

문서 수정

이 백서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
백서 업데이트	끊어진 링크가 수정되었고 전체적으로 편집상 변경이 많이 이루어졌습니다.	2023년 4월 25일
최초 게시	백서가 게시되었습니다.	2022년 10월 19일

고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공의 목적으로만 제공되고, (b) 사전 통지 없이 변경될 수 있는 현재 AWS 제품 및 관행을 나타내고, (c) AWS 및 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 약속이나 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 AWS 용어집을 참조하세요.

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