구매자 설명서

AWS Marketplace

AWS Marketplace: 구매자 설명서

Table of Contents

AWS Marketplace란 무엇인가요?

AWS Marketplace는 솔루션 빌드 및 비즈니스 운영에 필요한 타사 소프트웨어, 데이터 및 서비스를 찾아보고 구입, 배포 및 관리하는 데 사용할 수 있는 엄선된 디지털 카탈로그입니다. AWS Marketplace의 인기 카테고리에는 보안, 네트워킹, 스토리지, 기계 학습, IoT, 비즈니스 인텔리전스, 데이터베이스 및 DevOps 등 수천 가지 소프트웨어가 나열되어 있습니다. AWS Marketplace는 또한 유연한 요금 옵션 및 여러 배포 방법을 통해 소프트웨어 라이선싱 및 조달을 단순화합니다. 또한 AWS Marketplace에는 AWS Data Exchange에서 사용할 수 있는 데이터 제품이 포함되어 있습니다.

클릭 몇 번만으로 사전 구성된 소프트웨어를 빠르게 시작할 수 있으며 AMI(Amazon 머신 이미지) 및 SaaS(Software as a Service) 형식뿐만 아니라 기타 형식의 소프트웨어 솔루션을 선택할 수 있습니다. 또한 데이터 제품을 찾아보고 구독할 수 있습니다. 유연한 요금 옵션으로는 무료 평가판, 시간당, 월별, 연간, 다년 및 BYOL(Bring Your Own License)이 있습니다. 이러한 모든 요금 옵션은 하나의 소스에서 청구됩니다. AWS에서 청구 및 결제를 처리하며 요금은 AWS 청구서에 표시됩니다.

구매자(구독자) 또는 판매자(공급자)로서, 혹은 둘 다로서 AWS Marketplace를 사용할 수 있습니다. AWS 계정을 보유한 사람이라면 누구나 소비자로서 AWS Marketplace를 사용할 수 있으며, 판매자 등록도 가능합니다. 판매자는 독립 소프트웨어 공급자(ISV), 부가가치 리셀러 또는 AWS 제품 및 서비스와 호환되는 것을 제공하는 개인이 될 수 있습니다.

> **Note**
>
> 데이터 제품 공급자는 AWS Data Exchange 자격 요건을 충족해야 합니다. 자세한 내용은 AWS Data Exchange 사용 설명서의 AWS Data Exchange에서 데이터 제품 제공을 참조하세요.

AWS Marketplace의 모든 소프트웨어 제품은 큐레이션 프로세스를 거쳤습니다. 제품 페이지에는 제품 수가 1개 이상일 수도 있습니다. 판매자가 AWS Marketplace에서 제품을 제출할 때는 제품 가격과 이용 약관을 정의합니다. 구매자는 제공되는 제품에 설정된 요금 및 이용 약관에 동의합니다.

AWS Marketplace의 제품은 사용 요금이 없을 수도 있고 관련 요금이 부과될 수도 있습니다. 요금은 AWS 청구서에 포함되며, 사용자가 지불한 후에 AWS Marketplace가 판매자에게 지불합니다.

> **Note**
>
> 일부 미국 외 판매자로부터 구매할 경우 판매자로부터 세금 계산서를 받을 수도 있습니다. 자세한 내용은 Amazon Web Services 세금 도움말의 AWS Marketplace 판매자를 참조하세요.

제품은 여러 가지 형태로 제공됩니다. 예를 들어 AWS 계정을 사용하여 인스턴스화된 Amazon Machine Image(AMI)로 제품이 제공될 수도 있습니다. 또한 AWS CloudFormation 템플릿을 사용해 고객에게 제공하도록 제품을 구성할 수도 있습니다. 그 밖에도 제품은 ISV에서 제공하는 Software as a Service(SaaS) 제품이거나 웹 ACL, 규칙 집합 또는 AWS WAF 조건이 될 수도 있습니다.

ISV의 표준 최종 사용자 라이선스 계약(EULA)을 사용하거나 사용자 지정 가격 및 EULA가 포함된 비공개 제안을 통해 나열된 가격으로 소프트웨어 제품을 구매할 수 있습니다. 또한 표준 계약에 따라 시간 또는 사용량 경계를 지정하여 제품을 구매하는 것도 가능합니다.

제품 구독이 이루어지면 AWS Service Catalog를 사용하여 해당 제품을 복사하고 조직 내에서 제품에 액세스하고 사용하는 방법을 관리할 수 있습니다. 자세한 내용은 AWS Service Catalog 관리자 안내서의 포트폴리오에 AWS Marketplace 제품 추가를 참조하세요.

AWS Marketplace의 계약 구조

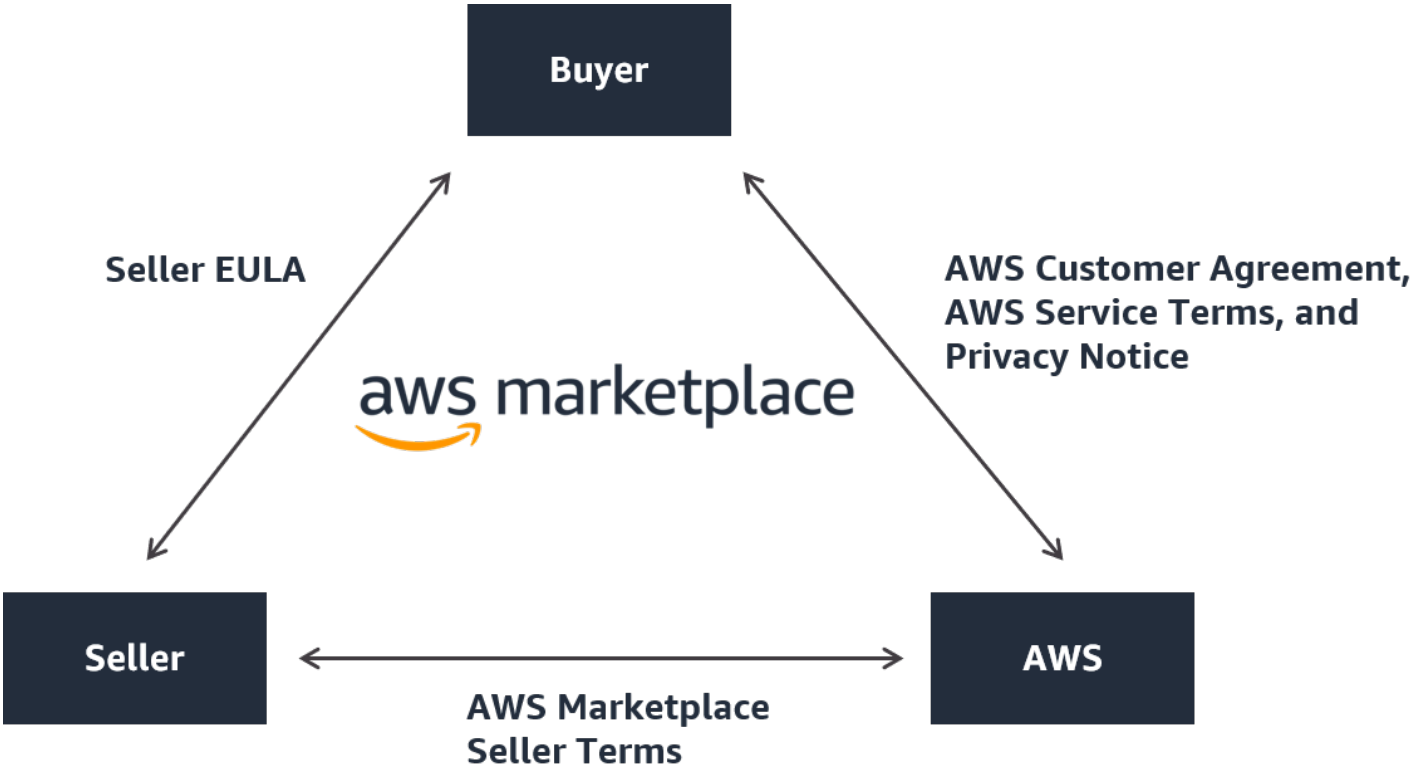
AWS Marketplace에서 판매되는 소프트웨어, 서비스 및 데이터 제품의 사용에는 구매자와 판매자가 체결한 계약이 적용됩니다. AWS는 이러한 계약의 당사자가 아닙니다.

구매자의 AWS Marketplace 사용에는 AWS 서비스 약관, AWS 이용계약 및 개인정보 취급방침이 적용됩니다.

판매자 계약에는 다음과 같은 내용이 포함됩니다.

- 판매자의 EULA는 AWS Marketplace의 공개 소프트웨어 리스팅에 대한 제품 목록 페이지에 있습니다. 많은 판매자가 AWS Marketplace 표준 계약(SCMP)을 기본 EULA로 사용합니다. SCMP를 비공개 제안 협상의 근거로 사용하고 수정 템플릿을 사용하여 SCMP를 수정할 수도 있습니다. 비공개 제안에는 당사자 간에 협상된 맞춤형 계약 조건도 포함될 수 있습니다.
- AWS Marketplace 판매자 약관은 AWS Marketplace에서 이루어지는 판매자의 활동을 통제합니다.

다음 그림은 AWS Marketplace의 계약 구조를 보여줍니다.



EULA 업데이트

판매자는 각 서비스형 소프트웨어(SaaS) 제품의 EULA를 업데이트할 수 있습니다. 이 업데이트가 EULA에 영향을 미치는 시기는 제안 유형과 요금 모델에 따라 다릅니다.

다음 표에는 SaaS 제품에 새 EULA가 적용되는 시기에 대한 정보가 나와 있습니다.

제안 유형	요금 모델	업데이트된 EULA가 적용되는 시기
퍼블릭	사용량	구독을 취소하고 다시 구독합니다.
퍼블릭	계약	현재 계약이 종료되고 새로운 공개 제안 계약으로 갱신됩니다.
퍼블릭	소비 계약	현재 계약이 종료되고 새로운 공개 제안 계약으로 갱신됩니다.

제안 유형	요금 모델	업데이트된 EULA가 적용되는 시기
비공개	사용량	현재 비공개 제안이 만료되고 새로운 공개 제안 계약으로 자동 갱신됩니다. 비공개 제안의 갱신은 비공개 제안에 따라 다릅니다.
비공개	계약	현재 비공개 제안이 만료되고 공개 제안 또는 새로운 비공개 제안을 다시 구독합니다. 비공개 제안의 갱신은 비공개 제안에 따라 다릅니다.
비공개	소비 계약	현재 비공개 제안이 만료되고 공개 제안 또는 새로운 비공개 제안을 다시 구독합니다. 비공개 제안의 갱신은 비공개 제안에 따라 다릅니다.

AWS Marketplace 표준 계약

제품 구매를 준비할 때, 관련 EULA 또는 표준 계약을 검토하세요. 많은 판매자가 리스팅에 AWS Marketplace 표준 계약(SCMP)을 제공합니다. AWS Marketplace에서는 구매자 및 판매자 커뮤니티와 협력하여 디지털 솔루션 사용을 관리하고 구매자와 판매자의 의무를 정의하기 위해 SCMP를 개발했습니다. 디지털 솔루션의 예로는 서버 소프트웨어, 서비스형 소프트웨어(SaaS), 인공 지능 및 기계 학습(AI/ML) 알고리즘 등이 있습니다.

각 구매에 대해 사용자 지정 EULA를 검토하는 대신 SCMP를 한 번만 검토하면 됩니다. SCMP를 사용하는 모든 제품의 계약 조건은 동일합니다.

판매자는 SCMP와 함께 다음 부록을 사용할 수도 있습니다.

- 보안 강화 부록 - 데이터 보안 요구 사항이 강화된 거래를 지원합니다.
- HIPAA 비즈니스 제휴 부록 - Health Insurance Portability and Accountability Act of 1996(HIPAA) 규정 준수 요구 사항이 적용되는 거래를 지원합니다.

표준 계약을 제공하는 제품 리스팅을 찾으려면 제품을 검색할 때 표준 계약 필터를 사용합니다. 비공개 제안의 경우 판매자에게 EULA를 SCMP로 바꾸고, 거래별 요구 사항을 지원하기 위해 필요하다면 합의된 수정안을 적용할 수 있느냐고 문의합니다.

자세한 내용은 AWS Marketplace의 표준 계약을 참조하세요.

AWS Marketplace를 구매자로 사용

구매자는 AWS Marketplace로 이동하여 Amazon Web Services에서 실행되는 제품을 검색, 필터링 및 탐색할 수 있습니다.

소프트웨어 제품을 선택하면 제품 페이지로 이동하게 됩니다. 제품 목록 페이지에는 제품, 요금, 사용량, 지원 및 제품 리뷰에 대한 정보가 담겨 있습니다. 소프트웨어 제품을 구독하려면 먼저 AWS 계정에 로그인한 후 EULA, 이용 약관, 그리고 구독을 사용자 지정할 때 사용할 수 있는 옵션이 기록된 구독 페이지로 이동합니다.

유럽, 중동 및 아프리카(터키 및 남아프리카공화국 제외)에 위치한 계정으로 EMEA 적격 판매자에게 AWS Marketplace 제품을 구매하는 행위는 Amazon Web Services EMEA SARL을 통해 이루어집니다.

특정 국가의 고객은 AWS Marketplace에서 제품을 구매할 때 Amazon Web Services EMEA SARL이 현지 부가가치세(VAT)를 부과합니다. 세금에 대한 자세한 내용은 AWS Marketplace 구매자 세금 도움말 페이지를 참조하세요.

Amazon Web Services EMEA SARL에 대한 자세한 내용은 Amazon Web Services EMEA SARL FAQ를 참조하세요.

EMEA 적격 판매자와 거래하는 고객은 Amazon Web Services EMEA SARL로부터 인보이스를 받습니다. 그 외의 거래는 계속해서 AWS Inc를 통해 진행됩니다. 자세한 내용은 제품 요금 납부를 참조하세요.

구독이 처리되면 실행 옵션, 소프트웨어 버전, 제품을 사용할 AWS 리전을 구성한 후 소프트웨어 제품을 시작할 수 있습니다. AWS Marketplace 웹 사이트의 내 Marketplace 소프트웨어, AWS Marketplace 또는 Amazon Elastic Compute Cloud(Amazon EC2) 콘솔 혹은 Service Catalog를 통해 제품을 찾거나 시작할 수도 있습니다.

AWS Marketplace를 통해 사용 가능한 제품 범주에 대한 자세한 내용은 제품 카테고리 섹션을 참조하세요.

AWS Marketplace의 소프트웨어 제품을 제공하는 방법에 대한 자세한 내용은 다음을 참조하세요.

- AMI 기반 서버 제품
- 컨테이너 제품
- 기계 학습 제품
- 전문 서비스 제품
- SaaS 제품
- 데이터 제품 - AWS Data Exchange 사용 설명서의 AWS Data Exchange란? 참조

AWS Marketplace 소프트웨어 및 서비스

AWS Marketplace는 데이터베이스, 애플리케이션 서버, 테스트 도구, 모니터링 도구, 콘텐츠 관리 및 비즈니스 인텔리전스 등 다수의 소프트웨어 카테고리로 구성되어 있습니다. 여기에서 잘 알려진 판매자의 상용 소프트웨어부터 널리 사용되는 오픈 소스 제품까지 선택할 수 있습니다. 원하는 제품을 찾으면 한 번의 클릭으로 해당 소프트웨어를 구입하여 자체 Amazon EC2 인스턴스에 배포할 수 있습니다. AWS CloudFormation을 사용하여 제품의 토폴로지를 배포할 수도 있습니다.

모든 AWS 고객은 AWS Marketplace에서 쇼핑할 수 있습니다. 소프트웨어 요금과 예상 인프라 요금은 웹사이트에 표시됩니다. 대부분의 소프트웨어는 AWS에 등록한 결제 수단을 사용하여 바로 구매할 수 있습니다. 소프트웨어 요금은 AWS 인프라 요금과 동일한 월별 청구서에 표시됩니다.

> **주의**
>
> - AWS Marketplace에는 서비스형 소프트웨어(SaaS) 제품과 서버 기반 제품을 포함하여 수많은 비즈니스 제품이 있습니다. 서버 기반 제품은 설정 및 유지보수를 위해 기술 지식이나 IT 지원이 필요할 수도 있습니다.
> - 자습서: Amazon EC2 Linux 인스턴스 시작하기의 정보와 자습서는 Amazon EC2 기본 사항을 배우는 데 도움이 될 것입니다.
> - AWS CloudFormation을 통해 AWS Marketplace 제품의 복잡한 토폴로지를 시작할 계획이라면 AWS CloudFormation 시작하기 항목이 유용한 AWS CloudFormation 기본 사항을 배우는 데 도움이 될 것입니다.

AWS Marketplace에는 다음과 같은 범주의 소프트웨어가 있습니다.

- 인프라 소프트웨어
- 개발자 도구

- 비즈니스 소프트웨어
- 기계 학습
- IoT
- 전문 서비스
- 데스크톱 애플리케이션
- 데이터 제품

자세한 내용은 제품 카테고리 섹션을 참조하세요.

각 주요 소프트웨어 카테고리에는 더 많은 하위 카테고리가 있습니다. 예를 들어 인프라 소프트웨어 카테고리에는 애플리케이션 개발, 데이터베이스 및 캐싱, 운영 체제 같은 하위 카테고리가 있습니다. 소프트웨어는 Amazon Machine Image(AMI) 및 서비스형 소프트웨어(SaaS)를 비롯한 7가지 제품 유형 중 하나로 제공됩니다. 소프트웨어 유형에 대한 자세한 내용은 제품 유형 섹션을 참조하세요.

필요한 소프트웨어를 쉽게 선택할 수 있도록 AWS Marketplace에서는 다음과 같은 정보를 제공합니다.

- 판매자 세부 정보
- 소프트웨어 버전
- 소프트웨어 유형(AMI 또는 SaaS) 및 AMI 관련 정보(해당되는 경우)
- 구매자 등급
- 가격
- 제품 정보

AWS Marketplace와 Amazon DevPay의 차이점

AWS Marketplace와 Amazon DevPay 사이에는 커다란 차이가 있습니다. 둘 다 고객이 AWS에서 실행되는 소프트웨어를 구매하는 데 유용하지만, AWS Marketplace는 Amazon DevPay보다 포괄적인 경험을 제공합니다. 소프트웨어 구매자에게 가장 커다란 차이점은 다음과 같습니다.

- AWS Marketplace는 Amazon.com과 좀 더 비슷한 쇼핑 경험을 제공하며, 사용 가능한 소프트웨어를 쉽게 검색할 수 있습니다.
- AWS Marketplace 제품은 Virtual Private Cloud(VPC)와 같은 다른 AWS 기능과 함께 작동하며 온디맨드 인스턴스뿐 아니라 Amazon Elastic Compute Cloud(Amazon EC2) 예약 인스턴스 및 스팟 인스턴스에서도 실행할 수 있습니다.

- AWS Marketplace는 Amazon Elastic Block Store(Amazon EBS)에서 지원되는 소프트웨어를 지원하지만, Amazon DevPay는 그렇지 않습니다.

그 밖에도 소프트웨어 판매자는 마케팅 활동은 물론이고 AWS Marketplace의 검색 용이성을 통해 이점을 얻기도 합니다.

구매자로 시작하기

다음 주제에서는 AWS Marketplace 구매자로 소프트웨어 제품을 시작하는 프로세스에 대해 간략하게 설명합니다.

주제

- 제품 구매
- 소프트웨어 시작
- 자습서: AMI 기반 소프트웨어 제품 구매
- 자세한 정보

데이터 제품 시작하기에 대한 자세한 내용은 AWS Data Exchange 사용 설명서의 AWS Data Exchange에서 데이터 제품 구독을 참조하세요.

제품 구매

AWS Marketplace에서 제품을 구매하는 것은 제품 목록 페이지에 표시된 제품 약관에 동의했음을 의미합니다. 여기에는 요금 조건 및 판매자의 최종 사용자 라이선스 계약(EULA)과 AWS 고객 계약에 따라 해당 제품을 사용할 것에 대한 동의도 포함됩니다. AWS Marketplace에서 수락한 제안에 대한 이메일 알림은 AWS 계정에 연결된 이메일 주소로 전송됩니다.

제품에 월별 요금이 적용되거나 구독 계약으로 제품을 구매하는 경우에는 구독과 동시에 요금이 청구됩니다. 구독은 해당 월의 남은 기간을 기준으로 비례 할당으로 계산됩니다. 다음 작업 중 하나를 수행하기 전에는 다른 요금이 부과되지 않습니다.

- Amazon Machine Image(AMI) 제품에서 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 시작합니다.
- AWS CloudFormation 템플릿을 사용하여 제품을 배포합니다.
- 판매자의 웹 사이트에서 제품을 등록합니다.

제품에 연간 구독 옵션이 적용된다면 구독과 동시에 연간 요금 전액이 청구됩니다. 연간 구독 요금은 제품 사용량을 보장하며, 최초 구독 날짜에서 1년이 지나면 구독 갱신이 필요합니다. 연간 구독 기간 종료 시 갱신하지 않으면 구독이 현재 시간 단위 요율의 시간당 구독으로 전환됩니다.

데이터 제품 구독에 대한 자세한 내용은 AWS Data Exchange 사용 설명서의 AWS Data Exchange에서 데이터 제품 구독을 참조하세요.

소프트웨어 시작

소프트웨어를 구매한 후에는 AWS Marketplace에서 1-Click 시작 보기를 사용하여 소프트웨어가 포함된 Amazon Machine Image(AMI)를 시작할 수 있습니다. AWS Management Console, Amazon Elastic Compute Cloud(Amazon EC2) 콘솔, Amazon EC2 API, AWS CloudFormation 콘솔을 비롯한 다른 Amazon Web Services(AWS) 관리 도구를 사용하여 시작할 수도 있습니다.

1-Click 시작 보기를 사용하면 단일 소프트웨어 인스턴스를 신속하게 검토하고 소프트웨어 판매자가 권장하는 설정으로 수정한 후 시작할 수 있습니다. EC2 콘솔을 사용해 시작 보기는 AWS Management Console, Amazon EC2 API 또는 기타 관리 도구를 사용하여 AMI를 시작하는 데 필요한 AMI 식별 번호와 기타 관련 정보를 쉽게 찾을 수 있습니다. 또한 EC2 콘솔을 사용해 시작 보기는 AWS Management Console에서 시작하는 것보다 더 많은 구성 옵션(예: 인스턴스 태그 지정)을 제공합니다.

토폴로지가 복잡한 AWS Marketplace 제품의 경우 사용자 지정 시작 보기를 보면 AWS CloudFormation 콘솔에서 적절한 AWS CloudFormation 템플릿으로 제품을 로드하는 CloudFormation 콘솔을 사용해 시작 옵션이 있습니다. 그런 다음, AWS CloudFormation 콘솔 마법사의 단계에 따라 해당 제품에 대한 AMI 클러스터 및 연결된 AWS 리소스를 생성할 수 있습니다.

자습서: AMI 기반 소프트웨어 제품 구매

다음 자습서에서는 AWS Marketplace에서 Amazon Machine Image(AMI) 제품을 구매하는 방법을 설명합니다.

단계

- 1단계: AWS 계정 생성
- 2단계: 소프트웨어 선택
- 3단계: 소프트웨어 구성
- 4단계: Amazon EC2에서 소프트웨어 시작
- 5단계: 소프트웨어 관리
- 6단계: 인스턴스 종료

1단계: AWS 계정 생성

AWS 계정에 로그인하지 않고도 AWS Marketplace 웹 사이트(https://aws.amazon.com/marketplace)를 탐색할 수 있습니다. 하지만 제품을 구독하거나 시작하려면 로그인해야 합니다.

AWS Marketplace 콘솔에 액세스하려면 AWS 계정에 로그인해야 합니다. AWS 계정 생성 방법에 대한 자세한 내용은 AWS Account Management 참조 가이드의 AWS 계정 생성을 참조하세요.

2단계: 소프트웨어 선택

소프트웨어를 선택하려면

1. AWS Marketplace 웹 사이트로 이동합니다.

   > **Note**
   >
   > 공개 AWS Marketplace 웹 사이트(https://aws.amazon.com/marketplace) 또는 AWS Management Console의 AWS Marketplace(https://console.aws.amazon.com/marketplace/home#/subscriptions)에서 새 인스턴스를 쇼핑, 구독 및 시작할 수 있습니다. 두 위치의 경험은 비슷합니다. 이 절차에서는 AWS Marketplace 웹 사이트를 사용하지만, 콘솔 사용 시 큰 차이점이 있습니다.

2. Shop All Categories(모든 카테고리 구매) 창에 선택할 수 있는 카테고리 목록이 있습니다. 그 밖에 가운데 창에서도 주요 소프트웨어를 선택할 수 있습니다. 이 자습서에서는 모든 카테고리 구매 창에서 콘텐츠 관리를 선택합니다.
3. 콘텐츠 관리 목록에서 Bitnami 및 Automattic 인증 WordPress를 선택합니다.
4. 제품 세부 정보 페이지에서 제품 정보를 살펴봅니다. 제품 세부 정보 페이지에는 다음과 같은 추가 정보가 포함되어 있습니다.

   - 구매자 등급
   - 지원 서비스
   - 주요 내용
   - 자세한 제품 설명
   - 각 AWS 리전의 인스턴스 유형에 대한 요금 정보(AMI인 경우)
   - 시작하는 데 도움이 되는 추가 리소스

5. Continue to Subscribe(구독 계속)를 선택합니다.
6. 아직 로그인하지 않았으면 AWS Marketplace에 로그인하라는 메시지가 표시됩니다. 이미 AWS 계정가 있으면 해당 계정을 사용하여 로그인할 수 있습니다. 아직 AWS 계정가 없으면 1단계: AWS 계정 생성 섹션을 참조하세요.
7. Bitnami 제안 약관을 읽은 다음, 계약 수락을 선택하여 구독 제안을 수락합니다.

8. 구독 작업이 완료될 때까지 잠시 시간이 걸릴 수 있습니다. 완료되면 구독 약관에 대한 이메일 메시지를 받게 되며, 그 후 계속 진행할 수 있습니다. 계속해서 구성을 선택하여 소프트웨어를 구성하고 시작합니다.

여기에서 제품 구독이란 제품 약관에 동의하였다는 것을 의미합니다. 제품에 월별 요금이 적용된다면 구독과 동시에 명시된 요금이 해당 월의 나머지 기간에 따라 비례 할당으로 계산되어 청구됩니다. 선택한 AMI로 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 시작하기 전에는 그 외의 다른 요금이 부과되지 않습니다.

> **Note**
>
> 제품 구독자의 경우 구독 중인 소프트웨어의 새 버전이 게시되면 계정으로 이메일 메시지가 전송됩니다.

3단계: 소프트웨어 구성

소프트웨어를 AMI로 선택했으므로, 다음 단계는 제공 방법, 버전 및 소프트웨어를 사용할 AWS 리전 선택을 포함하여 소프트웨어를 구성하는 것입니다.

소프트웨어를 구성하는 방법

1. 이 소프트웨어 구성 페이지에서 제공 방법으로 64비트(x86) Amazon Machine Image(AMI)를 선택합니다.
2. 소프트웨어 버전에 사용할 수 있는 최신 버전을 선택합니다.
3. 제품을 시작하려는 리전(예: 미국 동부(버지니아 북부))을 선택합니다.

   > **Note**
   >
   > 구성을 변경하면 화면 하단의 Ami Id가 업데이트됩니다. AMI ID의 형식은 ami-<identifier>(예: *ami-123example456*)입니다. 각 리전의 제품 버전마다 AMI가 다릅니다. 이 AMI ID를 통해 제품을 시작할 때 사용할 올바른 AMI를 지정할 수 있습니다. Ami 별칭은 자동화에 더 쉽게 사용할 수 있는 유사한 ID입니다.
   > AMI 별칭에 대한 자세한 내용은 AMI 별칭 사용 섹션을 참조하세요.

4. 계속해서 시작을 선택합니다.

4단계: Amazon EC2에서 소프트웨어 시작

Amazon EC2 인스턴스를 시작하려면 먼저 1-Click Launch로 시작할지, 혹은 Amazon EC2 콘솔을 사용해 시작할지 결정해야 합니다. 1-Click Launch는 보안 그룹, 인스턴스 유형 등 권장되는 기본 옵션으로 빠르게 시작할 때 유용합니다. 1-Click Launch에서는 예상되는 월 청구서도 확인할 수 있습니다. 그 밖에 Amazon Virtual Private Cloud(VPC)에서 시작하거나 스팟 인스턴스를 사용하는 등 더 많은 옵션을 원한다면 Amazon EC2 콘솔을 사용해 시작하는 것이 좋습니다. 다음은 제품을 구독한 후 1-Click Launch 또는 Amazon EC2 콘솔을 사용해 EC2 인스턴스를 시작하는 방법에 대한 절차입니다.

1-Click Launch를 사용하여 Amazon EC2 시작

1-Click Launch를 사용하여 Amazon EC2를 시작하는 방법

1. 이 소프트웨어 시작 페이지의 작업 선택 드롭다운에서 웹 사이트에서 시작을 선택하고 기본 설정을 검토합니다. 기본 설정을 변경하고 싶다면 다음과 같이 실행합니다.

   - EC2 인스턴스 유형 드롭다운 목록에서 인스턴스 유형을 선택합니다.
   - VPC 설정 및 서브넷 설정 드롭다운 목록에서 사용하려는 네트워크 설정을 선택합니다.
   - 보안 그룹 설정에서 기존 보안 그룹을 선택하거나, 판매자 설정에 따라 새로 생성을 선택하여 기본 설정을 수락합니다. 보안 그룹에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 Linux 인스턴스에 대한 Amazon EC2 보안 그룹을 참조하세요.
   - 키 페어를 확장한 후 가지고 있다면 기존 키 페어를 선택합니다. 키 페어가 없으면 키 페어를 생성하라는 메시지가 표시됩니다. Amazon EC2 키 페어에 대한 자세한 내용은 Amazon EC2 키 페어를 참조하세요.
2. 설정을 마쳤으면 시작하기를 선택합니다.

   새 인스턴스가 시작되고 Bitnami 및 Automattic 인증 WordPress 소프트웨어가 그 위에서 실행됩니다. 여기에서 인스턴스 세부 정보를 보거나, 다른 인스턴스를 만들거나, 소프트웨어의 모든 인스턴스를 볼 수 있습니다.

EC2 콘솔을 사용해 시작을 사용하여 Amazon EC2에서 시작

EC2 콘솔을 사용해 Amazon EC2를 시작하는 방법

1. EC2에서 시작 페이지에서 EC2 콘솔을 사용해 시작 보기를 선택한 다음, 버전 선택 목록에서 원하는 AMI 버전을 선택합니다.

2. Firewall Settings(방화벽 설정), Installation Instructions(설치 지침) 및 출시 정보를 살펴보고 Launch with EC2 Console(EC2 콘솔을 사용해 시작)을 선택합니다.
3. EC2 콘솔에서 인스턴스 요청 마법사를 사용하여 AMI를 시작합니다. Amazon EC2 Linux 인스턴스 시작하기의 지침에 따라 마법사를 진행합니다.

5단계: 소프트웨어 관리

언제든지 AWS Marketplace에서 AWS Marketplace 콘솔의 구독 관리 페이지를 사용하여 소프트웨어 구독을 관리할 수 있습니다.

소프트웨어를 관리하려면

1. AWS Marketplace 콘솔로 이동하여 구독 관리를 선택합니다.
2. 구독 관리 페이지에서 다음을 수행합니다.
   - 제품별 인스턴스 상태 보기
   - 당월 요금 보기
   - 새로운 인스턴스 시작
   - 인스턴스의 판매자 프로필 보기
   - 인스턴스 관리
   - 소프트웨어를 구성할 수 있도록 Amazon EC2 인스턴스에 직접 연결

6단계: 인스턴스 종료

더 이상 인스턴스가 필요하지 않다고 판단되면 인스턴스를 종료할 수 있습니다.

> **Note**
>
> 종료된 인스턴스는 다시 시작할 수 없습니다. 하지만 동일한 AMI 인스턴스를 추가로 실행할 수는 있습니다.

인스턴스를 종료하려면

1. AWS Marketplace 콘솔로 이동하여 구독 관리를 선택합니다.
2. 구독 관리 페이지에서 인스턴스를 종료하려는 소프트웨어 구독을 선택하고 관리를 선택합니다.

3. 특정 구독 페이지의 작업 드롭다운 목록에서 인스턴스 보기를 선택합니다.
4. 종료하려는 인스턴스가 있는 리전을 선택합니다. 그러면 Amazon EC2 콘솔이 열리고 해당 리전의 인스턴스가 새 탭에 표시됩니다. 필요한 경우 이 탭으로 돌아가서 종료할 인스턴스의 인스턴스 ID를 확인할 수 있습니다.
5. Amazon EC2 콘솔에서 인스턴스 ID를 선택하여 인스턴스 세부 정보 페이지를 엽니다.
6. 인스턴스 상태 드롭다운 목록에서 인스턴스 종료를 선택합니다.
7. 확인 메시지가 나타나면 종료를 선택합니다.

   인스턴스가 종료될 때까지 몇 분 정도 걸립니다.

자세한 정보

제품 카테고리 및 유형에 대한 자세한 내용은 제품 카테고리 및 제품 유형 항목을 참조하십시오.

Amazon EC2에 대한 자세한 내용은 Amazon Elastic Compute Cloud 설명서에서 서비스 설명서를 참조하십시오.

AWS에 대한 자세한 내용은 https://aws.amazon.com/을 참조하세요.

AWS 리전에서 지원되는 AWS Marketplace

소프트웨어 제품 판매자는 인스턴스 유형뿐만 아니라 소프트웨어를 제공할 AWS 리전을 선택합니다. 사용 가능한 모든 리전 및 의미 있는 모든 인스턴스 유형에서 제품을 사용할 수 있도록 하는 것이 좋습니다. AWS Marketplace 웹 사이트는 전 세계에서 사용할 수 있으며 다음과 같은 리전을 지원합니다.

- 북미
  - 미국 동부(오하이오)
  - 미국 동부(버지니아 북부)
  - 미국 서부(캘리포니아 북부)
  - 미국 서부(오리건)
  - AWS GovCloud(미국 동부)
  - AWS GovCloud(미국 서부)
  - 캐나다(중부)
  - 캐나다 서부(캘거리)

- 아프리카
  - 아프리카(케이프타운)

- 남아메리카
  - 남아메리카(상파울루)

- 유럽 중동 아프리카
  - 유럽(프랑크푸르트)
  - 유럽(아일랜드)
  - 유럽(런던)
  - 유럽(밀라노)
  - 유럽(파리)
  - 유럽(스페인)
  - 유럽(스톡홀름)
  - 유럽(취리히)

- 아시아 태평양
  - 아시아 태평양(홍콩)
  - 아시아 태평양(하이데라바드)
  - 아시아 태평양(자카르타)
  - 아시아 태평양(멜버른)
  - 아시아 태평양(뭄바이)
  - 아시아 태평양(오사카)
  - 아시아 태평양(서울)
  - 아시아 태평양(싱가포르)
  - 아시아 태평양(시드니)
  - 아시아 태평양(도쿄)

- 중동
  - 이스라엘(텔아비브)
  - 중동(바레인)
  - 중동(UAE)

데이터 제품이 지원되는 리전에 대한 자세한 내용은 AWS 일반 참조의 AWS Data Exchange 엔드포인트 및 할당량을 참조하세요.

제품 카테고리

AWS Marketplace 웹 사이트는 주요 범주로 구성되며, 각 주요 범주 아래에는 하위 범주가 있습니다. 범주 및 하위 범주를 기준으로 검색과 필터링이 가능합니다.

주제

인프라 소프트웨어

이 카테고리의 제품은 인프라 관련 솔루션을 제공합니다.

백업 및 복구

스토리지 및 백업 솔루션에 사용되는 제품

데이터 분석

데이터 분석에 사용되는 제품.

고성능 컴퓨팅

고성능 컴퓨팅 제품

마이그레이션

마이그레이션 프로젝트에 사용되는 제품

네트워크 인프라

네트워킹 솔루션을 개발하는 데 사용되는 제품

운영 체제

Linux 및 Windows 운영 체제 패키지

보안

인프라 보안 제품

스토리지

스토리지와 관련된 직무 역할에 사용되는 애플리케이션.

DevOps

이 카테고리의 제품은 개발자 및 개발자 팀을 위한 도구를 제공합니다.

애자일 수명 주기 관리

애자일 SDLM에 사용되는 제품.

애플리케이션 개발

애플리케이션 개발에 사용되는 제품

애플리케이션 서버

애플리케이션 개발에 사용되는 서버

애플리케이션 스택

애플리케이션 개발에 사용되는 스택

지속적 통합 및 지속적 전달(CI/CD)

CI/CD에 사용되는 제품.

코드형 인프라

인프라에 사용되는 제품.

문제 및 버그 추적

개발자 팀이 소프트웨어 버그를 추적 및 관리하는 데 사용되는 제품

모니터링(Monitoring)

작업 소프트웨어를 모니터링하는 데 사용되는 제품

로그 분석

로깅 및 로그 분석에 사용되는 제품

소스 제어

소스 제어를 관리하고 유지하는 데 사용되는 도구

테스트

소프트웨어 제품의 자동 테스트에 사용되는 제품

비즈니스 애플리케이션

이 카테고리의 제품은 비즈니스 운영에 효과적입니다.

블록체인

블록체인에 사용되는 제품.

협업 및 생산성

기업에서 협업을 촉진하는 데 사용되는 제품

고객 센터

조직의 고객 센터를 지원하는 데 사용되는 제품.

콘텐츠 관리

콘텐트 관리를 위한 제품

CRM

고객 관계 관리(CRM)를 위한 도구

전자 상거래

전자 상거래 솔루션을 제공하는 제품.

온라인 교육

온라인 교육 솔루션을 제공하는 제품.

HR

조직의 HR을 지원하는 데 사용되는 제품.

IT 비즈니스 관리

조직의 IT 비즈니스 관리를 지원하는 데 사용되는 제품.

비즈니스 인텔리전스

기업에서 비즈니스 인텔리전스를 촉진하는 데 사용되는 제품

프로젝트 관리

프로젝트 관리 도구

기계 학습

이 카테고리에 속하는 제품은 Amazon SageMaker에서 실행되는 기계 학습 알고리즘과 모델 패키지를 제공합니다.

ML 솔루션

기계 학습 솔루션

데이터 라벨링 서비스

데이터 라벨링 기능을 제공하는 제품

컴퓨터 비전

컴퓨터 비전 기능을 지원하는 제품

자연어 처리

자연어 처리 기능을 지원하는 제품

음성 인식

음성 인식 기능을 지원하는 제품

Text

텍스트 학습 기능을 지원하는 제품. 분류, 군집, 편집/처리, 임베딩, 생성, 문법/구문 분석, 식별, 이름 및 엔터티 인식, 감성 분석, 요약, 텍스트 투 스피치, 번역 등이 여기에 포함됩니다.

이미지

이미지 분석 기능을 지원하는 제품. 3D, 자막, 분류, 편집/처리, 임베딩/피처 추출, 생성, 문법/구문 분석, 필기 인식, 사람/얼굴, 객체 감지, 세그먼트 분리/픽셀 라벨링, 텍스트/OCR 등이 여기에 포함됩니다.

동영상

비디오 분석 기능을 지원하는 제품. 분류, 객체 감지, 편집/처리, 이상 탐지, 화자 식별, 모션, 재식별, 요약, 텍스트/자막, 추적 등이 여기에 포함됩니다.

오디오

오디오 분석 기능을 지원하는 제품. 화자 식별, 스피치 투 텍스트, 분류, 노래 식별, 세그먼트 분류 등이 여기에 포함됩니다.

구조

구조 분석 기능을 지원하는 제품. 분류, 군집, 차원 감소, 인수 분해 모델, 피처 엔지니어링, 순위, 회귀, 시계열 예측 등이 여기에 포함됩니다.

IoT

IoT 관련 솔루션을 개발하는 데 사용되는 제품

분석

IoT 솔루션에 사용되는 분석 제품

애플리케이션

IoT 솔루션 영역에 사용되는 애플리케이션 제품

디바이스 연결

디바이스 연결을 관리하는 데 사용되는 제품

디바이스 관리

디바이스를 관리하는 데 사용되는 제품

디바이스 보안

IoT 디바이스의 보안을 관리하는 데 사용되는 제품

산업용 IoT

산업 관련 IoT 솔루션을 제공하기 위한 제품

스마트 홈 및 시티

스마트 홈 및 스마트 시티 솔루션을 지원하는 제품

전문 서비스

이 카테고리의 제품은 AWS Marketplace 제품과 관련된 컨설팅 서비스를 제공합니다.

평가

현재 운영 환경을 평가하여 조직에 적합한 솔루션을 찾습니다.

구현

타사 소프트웨어의 구성, 설정 및 배포를 도와줍니다.

Managed Services

고객 대신 종합적으로 환경 관리.

Premium Support

요구 사항에 맞게 설계된 전문가의 지침 및 지원을 이용할 수 있습니다.

훈련

직원들이 모범 사례를 배울 수 있도록 전문가의 맞춤형 워크숍, 프로그램 및 교육 도구를 제공합니다.

데스크톱 애플리케이션

이 카테고리의 제품은 인프라 관련 솔루션을 제공합니다.

데스크톱 애플리케이션

일반적인 생산성이나 특정 직무 역할을 지원하는 데 사용되는 데스크톱 애플리케이션 및 유틸리티

AP 및 결제

지급 및 결제 계정을 담당하는 직무 역할에게 사용되는 애플리케이션

애플리케이션 및 웹

범용 및 웹 환경 애플리케이션

개발

개발에 사용되는 애플리케이션

비즈니스 인텔리전스

비즈니스 인텔리전스의 관리를 담당하는 직무 역할에게 사용되는 애플리케이션

CAD 및 CAM

CAD 및 CAM을 담당하는 직무 역할에게 사용되는 애플리케이션

GIS 및 매핑

GIS 및 매핑을 담당하는 직무 역할에게 사용되는 애플리케이션

일러스트레이션 및 디자인

일러스트레이션 및 디자인을 담당하는 직무 역할에게 사용되는 애플리케이션

미디어 및 인코딩

미디어 및 인코딩과 관련된 직무 역할에게 사용되는 애플리케이션

생산성 및 협업

생산성과 협업을 촉진하기 위한 애플리케이션

프로젝트 관리

프로젝트 관리자 직무 역할에게 사용되는 애플리케이션

보안/스토리지/아카이빙

보안, 스토리지 및 데이터 아카이빙과 관련된 직무 역할에게 사용되는 애플리케이션

유틸리티

다양한 직무 역할에게 사용되는 유틸리티 중심 애플리케이션

데이터 제품

이 카테고리의 제품은 파일 기반 데이터 세트입니다. 자세한 내용은 AWS Data Exchange 사용 설명서를 참조하세요.

업종

교육 및 연구

교육 및 연구 솔루션을 제공하는 데 목적을 둔 제품

금융 서비스

기업에서 금융 서비스를 촉진하는 제품

의료 및 생명과학

헬스케어 및 생명 과학 산업에 사용되는 제품

미디어 및 엔터테인먼트

미디어 관련 제품 및 솔루션

산업

산업 관련 제품 및 솔루션.

에너지

에너지 관련 제품 및 솔루션.

제품 유형

AWS Marketplace에는 인기 있는 오픈 소스 및 상용 소프트웨어뿐만 아니라 의 무료 및 유료 데이터 제품이 있습니다. 이러한 소프트웨어는 각 Amazon Machine Image(AMI), AWS CloudFormation 템플릿을 통해 배포되는 AMI 클러스터, 서비스형 소프트웨어(SaaS), 전문 서비스, AWS Data Exchange 데이터 제품 등 다양한 형태로 제공됩니다.

이러한 제품 유형에 대한 자세한 내용은 다음 주제를 참조하세요.

- AMI 기반 서버 제품(AMI 및 프라이빗 이미지 제품 포함)
- 컨테이너 제품
- 기계 학습 제품
- 전문 서비스 제품
- SaaS 제품
- 데이터 제품

AMI 기반 서버 제품

Amazon Machine Image(AMI)는 운영 체제와 AWS에서 실행되는 추가 소프트웨어를 포함한 서버 이미지를 말합니다.

AWS Marketplace에 나열된 소프트웨어는 Amazon Elastic Compute Cloud(Amazon EC2)에서만 실행할 수 있습니다. 다운로드는 불가능합니다.

AWS Marketplace에서는 AMI를 검색하거나(검색 추천 사용), 다른 고객이 제출한 제품 리뷰를 보거나, AMI를 구독하여 시작하거나, 구독을 관리할 수 있습니다. AWS Marketplace 제품은 모두 품질 확인을 거쳤으며 Amazon Web Services(AWS) 인프라에서 1-Click Launch 기능을 사용하도록 사전 구성되어 있습니다.

AMI 제품과 서비스형 소프트웨어(SaaS) 제품은 신뢰할 수 있는 판매자가 제공합니다. AMI 제품은 고객의 AWS 계정 내에서 실행됩니다. 따라서 소프트웨어 구성이나 소프트웨어를 실행하는 서버에 대한 제어 권한이 더욱 크지만 동시에 서버 구성 및 유지보수에 대한 책임도 커집니다.

AWS Marketplace 카탈로그는 오픈 소스 소프트웨어부터 잘 알려진 판매자의 상용 소프트웨어에 이르기까지 선별된 제품들로 구성되어 있습니다. AWS Marketplace의 여러 제품은 시간당 요금으로 구매할 수 있습니다.

AMI 카탈로그는 개발 팀을 비롯해 누구나 개발 중인 소프트웨어 또는 프로젝트를 광범위한 심사 없이 등록하거나 교환할 수 있는 커뮤니티 리소스입니다. 커뮤니티 AMI 카탈로그에 등록되는 제품은 잘 알려진 판매자의 제품이거나 그렇지 않을 수도 있으며, 일반적으로 추가 조사를 받지 않습니다.

AWS Marketplace 제품은 공급되는 AWS 리전마다 AMI가 하나씩 있습니다. 이러한 AMI들은 위치를 제외하면 모두 동일합니다. 또한 판매자가 최신 패치 및 업데이트로 자사 제품을 업데이트할 때 다른 AMI 세트를 제품에 추가하는 경우도 있습니다.

일부 AWS Marketplace 제품은 여러 AMI 인스턴스를 시작하기도 합니다. AWS CloudFormation 템플릿을 사용하여 클러스터로 배포되기 때문입니다. 이러한 인스턴스 클러스터는 CloudFormation 템플릿에서 추가로 구성되는 AWS 인프라 서비스까지 포함해 단일 제품 배포로 작동합니다.

AWS CloudFormation 템플릿

> **Important**
>
> AWS Marketplace는 AWS CloudFormation 템플릿을 사용하는 여러 Amazon Machine Image(AMI) 제품의 제공 방법을 2024년 8월에 중단할 예정입니다. CloudFormation을 사용하는 단일 AMI와 같이 CloudFormation을 사용하는 다른 AWS Marketplace 제품은 영향을 받지 않습니다.
> 2024년 8월까지 기존 구독자는 AWS Marketplace의 CloudFormation 템플릿을 사용하여 여러 AMI 제품의 새 인스턴스를 시작할 수 있습니다. 중단된 후에는 새 인스턴스를 시작할 수 없습니다. 이전에 시작하고 Amazon Elastic Compute Cloud(Amazon EC2)에서 실행 중인 기존 인스턴스는 영향을 받지 않으며 계속 실행됩니다.
> 궁금한 점은 AWS Support에 문의하세요.

AWS CloudFormation은 AWS 리소스를 모델링하고 설정하여 리소스 관리 시간을 줄이고 AWS에서 실행되는 애플리케이션에 더 많은 시간을 사용하도록 해 주는 서비스입니다. CloudFormation 템플릿은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 Amazon Relational Database Service(RDS) 데이터베이스 인스턴스와 같이 구매자가 원하는 다양한 AWS 리소스에 대해 설명합니다. CloudFormation은 이러한 리소스를 자동으로 프로비저닝하고 구성합니다. 자세한 내용은 AWS CloudFormation 시작하기를 참조하세요.

AWS CloudFormation 템플릿 사용

소프트웨어 판매자는 여러 AMI 인스턴스와 기타 AWS 리소스로 구성된 기본 배포 토폴로지를 정의할 수 있도록 AWS CloudFormation 템플릿을 제공할 수 있습니다. CloudFormation 템플릿이 제품과 함께 제공되는 경우에는 제품 목록 페이지에 배포 옵션으로 표시됩니다.

AMI를 사용하면 Amazon EC2 인스턴스 1개를 배포할 수 있습니다. 하지만 CloudFormation 템플릿을 사용하면 클러스터로 작동하는 여러 AMI 인스턴스를 Amazon RDS, Amazon Simple Storage Service(S3) 또는 기타 AWS 서비스 같은 AWS 리소스와 함께 단일 솔루션으로 배포할 수 있습니다.

주제

AWS Marketplace의 AMI 구독

AWS Marketplace의 일부 Amazon Machine Image(AMI) 기반 소프트웨어 제품은 연간 구독 요금 모델을 제공합니다. 이 요금 모델은 한 번만 선결제하면 이후 12개월 동안 시간당 사용료를 지불하지 않아도 됩니다. AWS Marketplace 소프트웨어 제품에 대한 연간 구독은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 하나에 적용할 수 있습니다.

> **Note**
>
> AMI 연간 시간당 요금의 경우 구매할 때 지정하는 인스턴스 유형만 연간 구독에 포함됩니다. 예: `t3.medium`. 다른 인스턴스 유형을 시작하면 활성 구독을 기준으로 해당 인스턴스 유형의 시간당 요금이 부과됩니다. 구매 후에는 연간 구독의 인스턴스 유형을 변경할 수 없습니다.

계속해서 시간당 요금제를 사용하여 AWS Marketplace 소프트웨어 제품을 시작하고 실행할 수도 있습니다. Amazon EC2 및 AWS의 기타 서비스 사용 요금은 AWS Marketplace 소프트웨어 제품의 구매 비용에 더하여 별도로 청구됩니다.

Amazon EC2 인스턴스 유형을 시간당 사용량으로 변경하면 가입한 절감형 플랜에 따라 Amazon EC2 인프라 요금이 청구됩니다. 하지만 AWS Marketplace의 AMI 라이선스는 자동으로 시간당 요금으로 변경됩니다.

AMI 시간당 제품이 연간 요금을 지원하지 않는 경우 구매자는 연간 구독을 구매할 수 없습니다. AMI 시간당 제품이 연간 요금을 지원하는 경우 구매자는 AWS Marketplace에서 제품 페이지로 이동하여 연

간 계약을 구매할 수 있습니다. 연간 계약마다 구매자는 인스턴스 하나를 시간당 요금 없이 실행할 수 있습니다. 계약은 인스턴스 유형에 따라 다릅니다.

계약 요금이 적용되는 AMI 제품

일부 판매자는 계약 요금 모델이 적용되는 공개 Amazon Machine Image(AMI) 기반 소프트웨어 제품을 제공합니다. 이 모델에서는 선택한 기간 동안 소프트웨어 제품에 액세스할 수 있는 개별 수량의 라이선스를 한 번 선결제하는 데 동의합니다. AWS 계정를 통해 요금이 미리 청구됩니다. 예를 들어 사용자 액세스 라이선스 10개와 관리 라이선스 5개 1년 사용권을 구매할 수 있습니다. 라이선스를 자동으로 갱신하도록 선택할 수 있습니다.

또한 일부 회사는 계약 요금 모델이 적용되는 비공개 AMI 기반 소프트웨어 제품을 제공합니다. 비공개 제안은 일반적으로 기간이 고정되어 있으며 기간을 변경할 수 없습니다.

AWS Marketplace의 제품 세부 정보 페이지에서 AMI 기반 소프트웨어 제품 계약을 구매할 수 있습니다. 이 옵션을 사용할 수 있으면 제품 세부 정보 페이지에서 제공 방법으로 계약 요금이 적용되는 AMI가 표시됩니다. 제품을 구매하면 계정 설정 및 구성을 위해 해당 제품의 웹 사이트로 이동됩니다. 이후부터는 정기 AWS 계정 청구서에 사용 요금이 표시됩니다.

계약 요금 공개 제안이 적용되는 AMI 제품 구독

계약 요금 모델이 적용되는 공개 제안 AMI 기반 제품을 구독하는 방법

1. AWS Marketplace에 로그인하고 계약 요금 모델이 적용되는 컨테이너 기반 소프트웨어 제품을 찾습니다.
2. 조달 페이지에서 요금 정보를 확인합니다.

   단위와 각 기간(개월 단위)의 요율을 확인할 수 있습니다.
3. 계속 구독하기를 선택하여 구독을 시작합니다.

   구독하지 않고 이 제품을 저장하려면 목록에 저장을 선택합니다.
4. 요금 정보를 검토하고 소프트웨어 제품 조건을 구성하여 계약을 생성합니다.

   a. 계약 기간을 1개월, 12개월, 24개월 또는 36개월 중에 선택합니다.
   b. 갱신 설정에서 계약 자동 갱신 여부를 선택합니다.
   c. 계약 옵션에서 각 단위의 수량을 선택합니다.

   총 계약 요금은 요금 세부 정보에 표시됩니다.

5. 선택을 마치면 Create Contract(계약 생성)를 선택합니다.

총 계약 요금이 AWS 계정로 청구됩니다. AWS License Manager에서 라이선스가 생성됩니다.

> **Note**
>
> 구독이 처리되고 AWS License Manager 계정에 소프트웨어 제품의 라이선스가 생성될 때까지 최대 10분이 걸릴 수 있습니다.

계약 요금 비공개 제안이 적용되는 AMI 제품 구독

계약 요금 모델이 적용되는 비공개 제안 AMI 기반 제품을 구독하는 방법

1. 구매자 계정으로 AWS Marketplace에 로그인합니다.
2. 비공개 제안을 봅니다.
3. 조달 페이지에서 요금 정보를 확인합니다.

   단위와 각 기간(개월 단위)의 요율을 확인할 수 있습니다.
4. 계속 구독하기를 선택하여 구독을 시작합니다.
5. 요금 정보를 검토하고 소프트웨어 제품 조건을 구성하여 계약을 생성합니다.

   계약 기간은 판매자가 이미 설정했으며 수정할 수 없습니다.
6. 계약 옵션에서 각 단위의 수량을 선택합니다.
7. 요금 세부 정보에서 총 계약 요금을 확인합니다.

   사용 가능한 다른 제안에서 혜택 보기를 선택하여 공개 제안을 볼 수도 있습니다.
8. 선택을 마치면 Create Contract(계약 생성)를 선택합니다.

> **Note**
>
> 구독이 처리되고 AWS License Manager 계정에 소프트웨어 제품의 라이선스가 생성될 때까지 최대 10분이 걸릴 수 있습니다.

소프트웨어 액세스

AMI 기반 소프트웨어 제품에 액세스하는 방법

1. AWS Marketplace 콘솔에서 구독 보기로 이동하여 소프트웨어 제품의 라이선스를 확인합니다.
2. 조달 페이지에서 다음을 수행합니다.

   a. 라이선스 관리를 선택하여 AWS License Manager에서 사용 권한을 보고, 액세스 권한을 부여하고, 사용 현황을 추적합니다.

   b. Continue to Configuration(구성 계속)을 선택합니다.
3. 시작 페이지에서 구성을 검토하고, 작업 선택에서 소프트웨어 시작 방법을 선택합니다.
4. 인스턴스 유형 선택에서 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 선택하고, 다음: 인스턴스 세부 정보 구성을 선택합니다.
5. 인스턴스 세부 정보 구성 페이지의 IAM 역할에서 AWS 계정의 기존 AWS Identity and Access Management(IAM) 역할을 선택합니다.

   IAM 역할이 없는 경우 수동으로 새 IAM 역할 생성 링크를 선택하고 지침을 따릅니다.

> **Note**
>
> 계약 요금이 적용되는 제품을 구매하면 AWS Marketplace가 AWS 계정에 라이선스를 생성하며, 소프트웨어에서 License Manager API를 사용하여 이 라이선스를 확인할 수 있습니다. AMI 기반 제품의 인스턴스를 시작하려면 IAM 역할이 필요합니다.
> IAM 정책에서 다음 IAM 권한이 필요합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "license-manager:CheckoutLicense",
            "license-manager:GetLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:ListReceivedLicenses"
         ],
         "Resource":"*"
      }
```

```
    ]
}
```

6. 인스턴스 세부 정보를 구성한 후에는 검토 및 시작을 선택합니다.
7. 인스턴스 시작 검토 페이지에서 기존 키 페어를 선택하거나 새 키 페어를 생성하고, 인스턴스 시작을 선택합니다.

   인스턴스 시작 개시 진행률 창이 나타납니다.
8. 인스턴스가 시작된 후, EC2 대시보드로 이동하여 인스턴스에서 인스턴스 상태가 실행 중으로 표시되는지 확인합니다.

생성된 라이선스 확인

생성된 라이선스를 확인하는 방법

1. AWS 계정로 AWS License Manager에 로그인합니다.
2. 권한 부여된 라이선스에서 권한 부여된 모든 라이선스를 확인합니다.
3. 검색 창에 제품 SKU, 수신자 또는 상태를 입력하여 라이선스를 검색합니다.
4. 라이선스 ID를 선택하고 라이선스 세부 정보를 확인합니다.
5. 발행자(AWS/Marketplace) 및 권한(라이선스가 애플리케이션 또는 리소스를 사용, 액세스 또는 소비할 수 있는 권한을 부여하는 단위)을 볼 수 있습니다.

기존 계약 수정

AMI 제품에 대한 기존 선결제 약정이 있는 경우 AWS Marketplace 구매자는 계약의 일부 조항을 수정할 수 있습니다. AMI 계약은 시간당 또는 연간 유연한 소비 요금(FCP) 제안과 달리 계약 조건 기반 제안을 통해 지원됩니다. 이 기능은 AWS License Manager와 통합된 애플리케이션에서만 사용할 수 있습니다. 구매자는 현재 계약에서 동일한 제안의 권한 내에서 추가 라이선스를 구매할 수 있습니다. 하지만 구매자는 계약에서 구매한 권한 수를 줄일 수 없습니다. 또한 판매자가 자동 구독 갱신 옵션을 활성화한 경우 구매자는 자동 구독 갱신을 취소할 수 있습니다.

> **Note**
>
> 유연한 결제 일정(FPS) 계약 제안은 수정할 수 없습니다. FPS 구매 계약에 대해서는 구매자가 변경할 수 있는 권한이 없습니다. 권한은 애플리케이션 또는 리소스를 사용, 액세스 또는 소비할 수 있는 권리입니다. FPS 제안은 변경할 수 없습니다.

구독 관리

1. AWS Marketplace 콘솔에서 구독 보기로 이동하여 소프트웨어 제품의 라이선스를 확인합니다.
2. 조달 페이지에서 라이선스 관리를 선택합니다.
3. 목록에서 약관 보기를 선택합니다.
4. 계약 옵션 섹션에서 화살표를 사용하여 권한을 늘립니다. 권한 개수를 구매한 권한 아래로 줄일 수 없습니다.
5. 계약 세부 정보 및 총 가격은 요금 세부 정보 섹션에 표시됩니다.

자동 구독 갱신을 취소하는 방법

1. AWS Marketplace 콘솔에서 구독 보기로 이동하여 소프트웨어 제품의 라이선스를 확인합니다.
2. 조달 페이지에서 라이선스 관리를 선택합니다.
3. 구독 페이지에서 갱신 설정 섹션을 찾습니다.
4. 취소와 관련된 이용 약관을 이해합니다.
5. 확인란을 선택하여 자동 갱신을 취소합니다.

측정이 지원되는 AMI 제품

AWS Marketplace에 등록된 일부 제품은 소프트웨어 애플리케이션에서 측정되는 사용량을 기준으로 요금이 청구됩니다. 측정되는 사용량으로는 데이터 사용량, 호스트/에이전트 사용량 또는 대역폭 사용량 등이 있습니다. 이러한 제품은 올바른 기능을 위해 추가 구성이 필요합니다. 사용량 측정 권한을 가지고 있는 IAM 역할이 시작할 때부터 AWS Marketplace Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결되어야 합니다. Amazon EC2용 IAM 역할에 대한 자세한 내용은 Amazon EC2의 IAM 역할을 참조하세요.

AMI 제품의 비용 할당 태그 지정

AWS Marketplace는 Amazon Machine Image(AMI) 기반 소프트웨어 제품의 비용 할당 태그 지정을 지원합니다. 신규 및 기존 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 태그는 해당 AWS Marketplace AMI 사용량에 따라 자동으로 채워집니다. 활성화된 비용 할당 태그를 사용하여 AWS Cost Explorer, AWS Cost & Usage Report, AWS Budgets 또는 기타 클라우드 비용 분석 도구를 통해 AMI 사용량을 확인하고 추적할 수 있습니다.

AMI를 제공한 공급업체는 제품 관련 정보를 기반으로 AMI 기반 제품의 요금 측정에 다른 사용자 지정 태그를 기록할 수도 있습니다. 자세한 내용은 비용 할당 태그 지정 섹션을 참조하세요.

태그를 이용하면 리소스를 정리할 수 있고, 비용 할당 태그를 이용하면 AWS 비용을 더 자세히 추적할 수 있습니다. 비용 할당 태그를 활성화하면 AWS은(는) 비용 할당 태그를 이용해 비용 할당 보고서에서 리소스 비용을 정리하기 때문에 사용자는 쉽게 AWS 비용을 분류하고 추적할 수 있습니다.

비용 할당 태그 지정은 과금 정보 및 비용 관리 콘솔에서 태그가 활성화된 시점 이후의 비용만 추적합니다. AWS 계정 소유자, AWS Organizations 관리 계정 소유자 및 적절한 권한이 있는 사용자만 계정의 과금 정보 및 비용 관리 콘솔에 액세스할 수 있습니다. 비용 할당 태그 사용 여부는 청구되는 금액에 영향을 주지 않습니다. 비용 할당 태그 사용 여부는 AMI 기반 소프트웨어 제품의 기능에 영향을 주지 않습니다.

여러 인스턴스에서 단일 AMI에 대한 비용 할당 태그 추적

AWS Marketplace AMI 구독에 대해 시작되는 각 Amazon EC2 인스턴스는 AWS Cost & Usage Report에 해당 AWS Marketplace 소프트웨어 사용 항목이 있습니다. AWS Marketplace 사용량에는 해당 Amazon EC2 인스턴스에 적용된 특정 태그가 항상 반영됩니다. 따라서 인스턴스 수준에서 할당된 다른 값을 기준으로 AWS Marketplace 사용 비용을 구별할 수 있습니다.

또한 태그 기반 사용 비용을 합산하면 Cost Explorer 또는 AWS Cost & Usage Report에서 청구서에 반영된 AMI 소프트웨어 사용 비용과 같습니다.

비용 할당되고 태그 지정된 인스턴스를 사용하여 예산 찾기

과금 정보 및 비용 관리 콘솔의 여러 Amazon EC2 인스턴스에 대한 비용 할당 태그에서 활성 예산을 이미 필터링한 경우 예산을 모두 찾는 것이 어려울 수 있습니다. 다음 Python 스크립트는 현재 AWS 리전의 AWS Marketplace에서 Amazon EC2 인스턴스를 포함하는 예산 목록을 반환합니다.

이 스크립트를 사용하여 예산에 미치는 잠재적 영향과 이 변경으로 인해 오버런이 발생할 수 있는 위치를 파악할 수 있습니다. 청구되는 금액은 변경되지 않지만 예산에 영향을 줄 수 있는 비용 할당이 더 정확하게 반영됩니다.

```
#! /usr/bin/python

import boto3

session = boto3.Session()
b3account=boto3.client('sts').get_caller_identity()['Account']
print("using account {} in region {}".format(b3account,session.region_name))


def getBudgetFilters(filtertype):
    '''
    Returns budgets nested within the filter values [filter value][budeget name].
    The filtertype is the CostFilter Key such as Region, Service, TagKeyValue.
    '''
    budget_client = session.client('budgets')
    budgets_paginator = budget_client.get_paginator('describe_budgets')
    budget_result = budgets_paginator.paginate(
        AccountId=b3account
    ).build_full_result()
    returnval = {}
    if 'Budgets' in budget_result:
        for budget in budget_result['Budgets']:
            for cftype in budget['CostFilters']:
                if filtertype == cftype:
                    for cfval in budget['CostFilters'][cftype]:
                        if cfval in returnval:
                            if not budget['BudgetName'] in returnval[cfval]:
                                returnval[cfval].append(budget['BudgetName'])
                        else:
                            returnval[cfval] = [ budget['BudgetName'] ]
    return returnval

def getMarketplaceInstances():
    '''
    Get all the AWS EC2 instances which originated with AWS Marketplace.
    '''
    ec2_client = session.client('ec2')
    paginator = ec2_client.get_paginator('describe_instances')
    returnval = paginator.paginate(
        Filters=[{
            'Name': 'product-code.type',
            'Values': ['marketplace']
        }]
```

```
    ).build_full_result()
    return returnval


def getInstances():
    mp_instances = getMarketplaceInstances()
    budget_tags = getBudgetFilters("TagKeyValue")
    cost_instance_budgets = []
    for instance in [inst for resrv in mp_instances['Reservations'] for inst in
 resrv['Instances'] if 'Tags' in inst.keys()]:
        for tag in instance['Tags']:
            # combine the tag and value to get the budget filter string
            str_full = "user:{}${}".format(tag['Key'], tag['Value'])
            if str_full in budget_tags:
                for budget in budget_tags[str_full]:
                    if not budget in cost_instance_budgets:
                        cost_instance_budgets.append(budget)
    print("\r\nBudgets containing tagged Marketplace EC2 instances:")
    print( '\r\n'.join([budgetname for budgetname in cost_instance_budgets]) )


if __name__ == "__main__":
    getInstances()
```

출력 예

```
Using account 123456789012 in region us-east-2

Budgets containing tagged Marketplace EC2 instances:
EC2 simple
MP-test-2
```

관련 주제

자세한 정보는 다음 주제를 참조하세요.

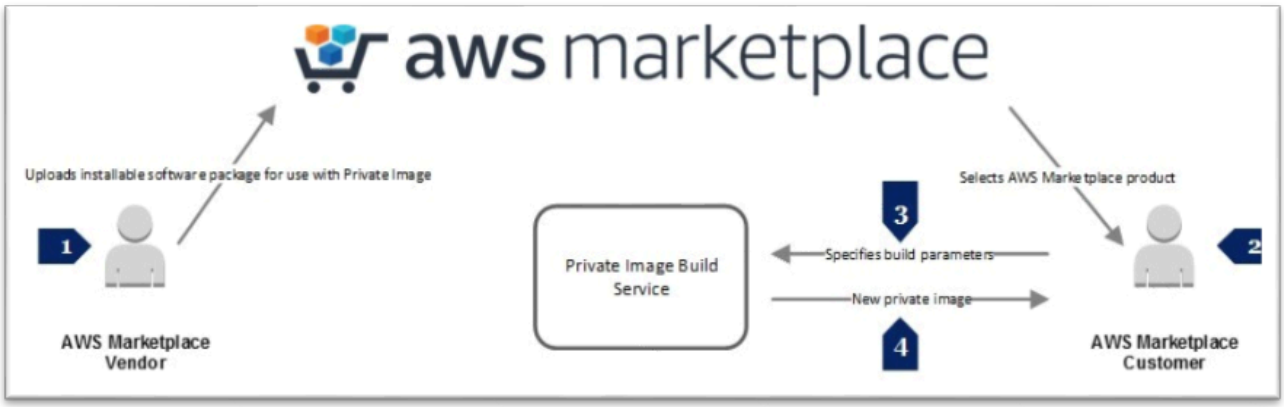
- AWS Billing 사용 설명서의 비용 할당 태그 사용
- AWS Billing 사용 설명서의 AWS에서 생성하는 비용 할당 태그 활성화
- Linux 인스턴스용 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태그 지정

프라이빗 이미지 빌드

> **Important**
>
> AWS Marketplace는 2024년 4월에 프라이빗 이미지 빌드 제공 방법을 중단할 예정입니다. 2024년 4월까지 기존 프라이빗 이미지 빌드 구독자는 프라이빗 이미지 빌드 소프트웨어를 사용하여 새 골든 Amazon Machine Image(AMI)를 빌드하거나 골든 AMI를 업그레이드할 수 있습니다. 중단된 후에는 프라이빗 이미지 빌드 소프트웨어를 사용하여 자체 AMI를 빌드하거나 업그레이드할 수 없습니다. 이전에 프라이빗 이미지 빌드를 사용하여 빌드한 기존 AMI는 영향을 받지 않습니다. 즉, 프라이빗 이미지 빌드를 사용하여 빌드한 AMI는 계속해서 요금이 청구되고 Amazon Elastic Compute Cloud(Amazon EC2)를 사용하여 시작할 수 있으며 활성 인스턴스는 지금처럼 계속 실행됩니다.
>
> 또한 이전에는 프라이빗 이미지 빌드로만 제공되었던 소프트웨어를 이제는 독립형 AMI 이행 옵션을 통해 사용할 수 있으며, 이 옵션은 중단되지 않습니다. 프라이빗 이미지 빌드가 중단된 후에도 독립형 AMI를 기존 프라이빗 이미지 빌드 구독과 함께 계속 사용할 수 있습니다. 궁금한 점은 AWS Support에 문의하십시오.

AWS Marketplace 프라이빗 이미지 빌드는 AWS Marketplace에서 설치 가능한 소프트웨어 제품을 구매한 후 해당 제품을 골드 이미지에, 혹은 AWS 계정에서 사용할 수 있는 이미지 중에서 선택한 AMI에 설치할 수 있는 서비스입니다. 이번 단원에서 언급하는 골드 이미지는 기본 운영 체제(OS)가 포함되어 있으면서, 동시에 이미지에서 시작되는 각 서버가 고객이 정의하는 IT 표준을 따를 수 있도록 수정된 서버 이미지를 말합니다. 설치할 AWS Marketplace 소프트웨어와 빌드에 사용할 기본 AMI를 선택합니다. 그런 다음 AWS Marketplace 이미지 빌드 서비스를 사용해 새로운 AMI를 빌드한 후 AWS 계정에서만 사용할 수 있는 프라이빗 이미지로 만듭니다.

이 서비스는 AWS Marketplace 제품을 고객의 IT 표준에 따른 기본 운영 체제에서 실행할 수 있다는 점에서 고객의 내부 보안, 규정 준수 및 관리 요건을 해결하는 데 매우 효과적입니다.



AWS Marketplace 프라이빗 이미지 빌드 서비스에 참여하는 판매자는 특정 OS 플랫폼, OS 및 OS 버전에 따라 설치할 수 있는 버전의 제품을 생성합니다. 판매자가 자사의 제품에 사용할 소프트웨어 패키지 세트를 제출하면 AWS Marketplace 이미지 빌드 서비스는 지정된 OS에 제품을 설치하고 스캔한 후 AWS Marketplace에 제품을 게시합니다. AWS Marketplace 프라이빗 이미지 빌드를 지원하는 제품을 구매하면 기존 AMI를 선택하여 새로운 프라이빗 이미지를 빌드할 수 있습니다. AWS Marketplace 이미지 빌드 서비스를 사용하여 새 이미지를 빌드한 후에는 Amazon EC2 콘솔에서 해당 이미지를 본인 소유의 이미지로 사용할 수 있습니다. AWS Marketplace 웹 사이트를 사용하여 이미지를 빌드할 수 있으며, AWS Marketplace 이미지 빌드 서비스 API를 사용하는 방법도 있습니다.

제품에 따라 1~2시간이 소요되는 빌드 프로세스에서 AWS 서비스를 사용하면 소프트웨어 및 인프라 요금이 발생합니다. 하지만 AWS Marketplace 이미지 빌드 서비스를 사용하여 프라이빗 이미지를 생성하면 추가 요금이 없습니다. 이미지가 빌드된 후에는 제품을 사용할 때까지는 제품 또는 AWS 리소스 사용 요금이 발생하지 않습니다.

AWS Marketplace 프라이빗 이미지 빌드 서비스는 AWS Identity and Access Management(IAM)를 사용하여 프라이빗 이미지를 빌드하고 볼 수 있는 제한적 권한을 최종 사용자에게 부여하는 IAM 역할과 정책을 생성합니다. 사전 필수 단계를 마치려면 관리자 권한이 필요합니다.

사전 조건 단계 완료

> **Important**
>
> AWS Marketplace는 2024년 4월에 프라이빗 이미지 빌드 제공 방법을 중단할 예정입니다. 제공 방법은 중단되기 전까지는 기존 구독자만 사용할 수 있습니다. 자세한 내용은 프라이빗 이미지 빌드를 참조하세요.

여기에서 설명하는 사전 조건 단계를 완료하려면 AWS Identity and Access Management(IAM)를 구성할 수 있는 관리자 권한이 있어야 합니다. 그래야만 프라이빗 이미지를 빌드할 수 있는 권한을 다른 사용자에게 부여할 수 있습니다. IAM 정책과 역할이 생성되었으면, 해당 정책과 역할을 그룹(또는 사용자) 계정에 연결할 수 있으며, 연결된 사용자는 프라이빗 이미지를 빌드할 수 있습니다.

IAM은 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스입니다. IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어합니다. 먼저 자격 증명(사용자, 그룹 및 역할)을 생성한 후 개별 사용자가 아닌 그룹을 관리할 수 있도록 사용자를 그룹에 추가합니다. IAM 역할은 각 자격 증명이 AWS에서 할 수 있는 것과 없는 것을 결정할 수 있는 권한 정책을 갖춘 자격 증명이라는 점에서 사용자와 유사합니다. 하지만 역할은 연결되어 있는 자격 증명(암호 또는 액세스 키)이 없습니다. 역할은 한 사람과만 연관되는 것이 아니라 그 역할이 필요한 사람이면 누구든지 맡을

수 있도록 고안되었습니다. 사용자는 한 가지 역할을 맡아서 특정 작업을 위한 다른 권한을 임시로 얻을 수 있습니다.

IAM의 액세스 관리 서비스는 사용자 또는 다른 엔터티가 계정에서 할 수 있는 작업을 정의하는 데 유용하며, 종종 권한 부여라고도 불립니다. 권한은 정책을 통해 부여됩니다. 정책은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 AWS의 엔터티입니다. AWS는 사용자와 같은 보안 주체가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지를 결정합니다. 정책은 JSON 문서로 AWS에 저장되며 자격 증명 기반 정책으로 보안 주체에 연결되거나 리소스 기반 정책으로 리소스에 연결됩니다. 권한 정책을 정의하고 정책을 그룹에 할당하여 권한을 부여할 수 있습니다.

자격 증명 기반 정책은 사용자, 역할 또는 그룹 같은 보안 주체(또는 자격 증명)에 연결할 수 있는 권한 정책입니다. 리소스 기반 정책은 Amazon Simple Storage Service(Amazon S3) 버킷 같은 리소스를 연결할 수 있는 JSON 정책 문서입니다. 자격 증명 기반 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. 자격 증명 기반 정책은 AWS 관리형 정책, 고객 관리형 정책 및 인라인 정책으로 분류할 수 있습니다.

리소스 기반 정책은 지정된 보안 주체가 해당 리소스에 대해 수행할 수 있는 작업 및 이에 관한 조건을 제어합니다. 리소스 기반 정책은 인라인 정책이며, 관리형 리소스 기반 정책은 없습니다. IAM 자격 증명이 기술적으로 AWS 리소스라고 해도 리소스 기반 정책을 IAM 자격 증명에 연결할 수는 없습니다. IAM에서는 자격 증명 기반 정책을 사용해야 합니다. 신뢰 정책은 역할을 위임할 수 있는 보안 주체를 정의하는 역할에 연결된 리소스 기반 정책입니다. IAM에서 역할을 생성하면 해당 역할에 두 정책이 있어야 합니다. 하나는 누가 역할을 맡을지 나타내는 신뢰 정책이고, 나머지 하나는 해당 역할을 사용해 할 수 있는 작업을 나타내는 권한 정책입니다. 역할의 신뢰 정책에 계정을 추가하는 것은 신뢰 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 신뢰받는 계정의 어떤 사용자도 그 계정에 대한 관리자가 해당 사용자에게 역할을 수임할 수 있는 권한을 부여할 때까지 역할을 수임할 수 없도록 기본 설정되어 있습니다.

AWS Marketplace 이미지 빌드 서비스는 두 가지 IAM 역할을 사용하며, 역할마다 권한 정책과 신뢰 정책이 있습니다. 사용자에게 AWS Marketplace 웹 사이트에 액세스하여 프라이빗 이미지를 빌드할 수 있도록 허용하는 경우에는 해당 사용자 역시 프라이빗 이미지를 생성하고 확인할 때 필요한 역할을 나열하고 할당할 수 있는 IAM 권한이 필요합니다.

관리자는 필요한 역할 2개와 여기에 연결할 정책을 생성합니다. 첫 번째 역할은 이미지 빌드 프로세스에서 생성된 인스턴스에 연결되는 인스턴스 프로파일입니다. 인스턴스 프로파일이란 IAM 역할을 위한 컨테이너로서 인스턴스 시작 시 Amazon EC2 인스턴스에 역할 정보를 전달하는 데 사용됩니다. 두 번째는 AWS Systems Manager 및 Amazon EC2에 대한 액세스 권한을 부여하는 IAM 역할입니다. 인스턴스 프로파일을 구성하려면 먼저 필요한 권한을 부여하는 권한 정책을 연결합니다. 그런 다음, IAM 역할이 역할 위임을 위해 Amazon EC2 및 Systems Manager에 대한 권한을 부여할 수 있도록 신뢰 정책을 편집합니다.

인스턴스 프로파일 역할 생성

IAM 콘솔에서 인스턴스 프로파일 역할을 생성하는 방법

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할과 역할 생성을 차례대로 선택합니다.
3. 신뢰할 수 있는 엔터티 유형 선택(Select type of trusted entity에서 AWS 서비스를 선택합니다.
4. Choose the service that will use this role(이 역할을 사용할 서비스 선택)에서 EC2와 Next: Permissions(다음: 권한)를 차례대로 선택합니다.
5. 정책 생성에서 Next: Review(다음: 검토)를 선택합니다.
6. 역할 이름에 이 역할의 목적을 식별하는 데 도움이 되는 역할 이름이나 역할 이름 접두사를 입력합니다(예: **`MyInstanceRole`**). 역할 이름은 AWS 계정에서 고유해야 합니다.
7. 역할을 검토한 다음 [Create role]을 선택합니다.
8. 역할 페이지에서 방금 생성한 역할을 선택합니다.
9. 권한에서 Add inline policy(인라인 정책 추가)를 선택합니다.
10. JSON 탭을 선택하고 모든 텍스트를 다음 `InstanceRolePermissionsPolicy` 텍스트로 바꿉니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:GetDocument",
                "ssm:GetManifest",
                "ssm:GetParameters",
                "ssm:ListAssociations",
                "ssm:ListInstanceAssociations",
                "ssm:PutConfigurePackageResult",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "ec2messages:AcknowledgeMessage",
                "ec2messages:DeleteMessage",
                "ec2messages:FailMessage",
                "ec2messages:GetEndpoint",
                "ec2messages:GetMessages",
                "ec2messages:SendReply"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeInstanceStatus"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> 이 프로세스를 시작하기 전에, S3 버킷 *DOC-EXAMPLE-BUCKET*을 생성해야 합니다.

11. Review policy(정책 검토)를 선택합니다.
12. 정책 이름에 해당 정책의 목적을 식별하는 데 도움이 될 수 있는 이름(예: **MyInstanceRolePolicy**)을 입력하고 정책 생성을 선택합니다.

역할에 대한 신뢰 관계를 편집하는 방법

1. 역할 페이지에서 방금 생성한 역할을 선택합니다.
2. 신뢰 관계 탭을 선택한 후 Edit trust relationship(신뢰 관계 편집)을 선택합니다.

3. 정책 문서 텍스트 상자에 있는 텍스트를 모두 선택하고 다음 `InstanceRoleTrustPolicy` 텍스트로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com",
          "ec2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 신뢰 정책 업데이트(Update Trust Policy)를 선택합니다.

AWS Systems Manager 자동화 역할 생성

AWS Systems Manager 자동화 역할을 생성하는 방법

1. IAM 콘솔의 탐색 창에서 역할과 역할 생성을 차례대로 선택합니다.
2. 신뢰할 수 있는 엔터티 유형 선택(Select type of trusted entity에서 AWS 서비스를 선택합니다.
3. Choose the service that will use this role(이 역할을 사용할 서비스 선택)에서 EC2와 Next: Permissions(다음: 권한)를 차례대로 선택합니다.
4. 정책 생성에서 Next: Review(다음: 검토)를 선택합니다.
5. 역할 이름에 이 역할의 목적을 식별하는 데 도움이 되는 역할 이름이나 역할 이름 접두사를 입력합니다(예: **`MyAutomationRole`**). 역할 이름은 AWS 계정에서 고유해야 합니다.
6. 역할을 검토한 다음 [Create role]을 선택합니다.
7. 역할 페이지에서 방금 생성한 역할을 선택합니다.
8. 권한에서 Add inline policy(인라인 정책 추가)를 선택합니다.
9. JSON 탭을 선택하고 모든 텍스트를 다음 `AutomationRolePermissionsPolicy` 텍스트로 바꿉니다.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:CreateImage",
                "ec2:DescribeImages",
                "ec2:StartInstances",
                "ec2:RunInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:CreateTags",
                "ec2:DescribeTags"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "{{ Instance Profile }}"
            ],
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> `{{ Instance Profile }}`을 앞에서 생성한 인스턴스 정책 역할의 Amazon 리소스 이름(ARN)으로 바꿔야 합니다. IAM 관리 콘솔에서 해당 역할을 찾아 선택하십시오. 역할의 요약 페이지에서 가장 먼저 나열되는 항목은 역할 ARN(예: `arn:aws:iam::123456789012:role/MyInstanceRole`)입니다.

역할에 대한 신뢰 관계를 편집하는 방법

1. 역할 페이지에서 방금 생성한 역할을 선택합니다.
2. 신뢰 관계 탭을 선택한 후 Edit trust relationship(신뢰 관계 편집)을 선택합니다.
3. 정책 문서 텍스트 상자에 있는 모든 텍스트를 다음 `InstanceRoleTrustPolicy` 텍스트로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com",
          "ec2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 신뢰 정책 업데이트(Update Trust Policy)를 선택합니다.

이제 역할 2개와 여기에 연결된 정책을 생성하였습니다. 생성된 역할과 정책은 프라이빗 이미지 빌드 프로세스에서 사용됩니다.

정책을 사용하여 AWS Marketplace 웹 사이트에 액세스

대부분의 조직에서는 사용자가 루트 계정 보안 인증 정보를 사용하여 로그인하는 것을 허용하지 않습니다. 그 대신 조직 내 특정 인물만 수행할 수 있는 역할 또는 작업에 따라 제한된 권한만 있는 사용자를 생성합니다. AWS Marketplace는 AWS Marketplace 도구에서 작업할 수 있는 두 가지 기본 IAM 관리형 정책을 제공합니다. 이 두 가지 관리형 정책을 사용해 아래와 같은 작업을 수행할 수 있는 권한을 부여하십시오.

- `AWSMarketplaceFullAccess` - IAM 소프트웨어를 구독 및 구독 취소할 수 있는 기능을 제공하고, 사용자가 AWS Marketplace 사용자 소프트웨어 페이지에서 AWS Marketplace 소프트웨어 인스턴스를 관리할 수 있도록 허용하고, Amazon EC2에 대한 관리자 액세스 권한을 부여합니다.
- `AWSMarketplaceRead-only` - AWS 구독을 검토하는 기능을 제공합니다.

`AWSMarketplaceFullAccess` 관리형 정책을 사용자, 그룹 또는 역할에 추가하여 AWS Marketplace 웹 사이트에 액세스하고 AWS Marketplace 프라이빗 이미지 빌드와 연결된 작업을 수행하는 데 필요한 모든 권한을 부여할 수 있습니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가합니다.

- AWS IAM Identity Center의 사용자 및 그룹:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따르세요.
- 자격 증명 공급자를 통해 IAM에서 관리되는 사용자:

  아이덴티티 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기(연합)의 지침을 따르세요.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 IAM 사용자의 역할 생성의 지침을 따르세요.
  - (권장되지 않음) 정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

선택한 그룹 또는 역할에 속한 사용자나 구성원은 다음에 AWS Marketplace 웹 사이트에 액세스할 때 프라이빗 이미지 빌드 프로세스와 관련된 작업을 수행할 수 있습니다.

프라이빗 이미지 빌드

> **Important**
>
> AWS Marketplace는 2024년 4월에 프라이빗 이미지 빌드 제공 방법을 중단할 예정입니다. 제공 방법은 중단되기 전까지는 기존 구독자만 사용할 수 있습니다. 자세한 내용은 프라이빗 이미지 빌드를 참조하세요.

프라이빗 이미지를 생성할 때, AWS Marketplace에서 소프트웨어 패키지를 선택하고, Amazon Elastic Compute Cloud(Amazon EC2) 콘솔에서 새 프라이빗 이미지를 생성할 때 사용할 기본 Amazon Machine Image(AMI)를 선택합니다. 빌드 프로세스를 시작하려면 먼저 다음 정보를 제공할 수 있는 AWS 환경을 구성해야 합니다.

- AWS Marketplace 제품을 설치할 기본 이미지의 AMI ID.
- 빌드 로그를 저장할 Amazon Simple Storage Service(S3) 버킷의 이름. S3 버킷은 AMI를 사용할 수 있는 AWS 리전에 속해야 합니다.
- 패키지를 설치할 때 사용할 Amazon EC2 인스턴스 프로파일(이전 단원 참조).
- 이미지 생성 프로세스에서 AMI를 생성할 때 사용할 AWS Identity and Access Management(IAM) 자동화 역할(이전 단원 참조).
- 새 프라이빗 이미지 이름.

AWS 서비스 사용 경험이 있는 분들은 아마도 AWS 리전을 선택하고, Amazon EC2 대시보드에서 AMI ID를 찾고, Amazon S3 버킷을 작업하는 데 익숙하실 것입니다.

프라이빗 이미지 빌드를 지원하는 제품을 찾으려면 AWS Marketplace 제품 검색 페이지로 이동한 다음, 제공 방법 검색 필터에서 프라이빗 Amazon 머신 이미지(AMI)를 선택합니다. 제품 세부 정보 페이지에서 구매, 구성 및 실행 옵션을 설정합니다. 빌드할 제품이 AWS 계정에 추가됩니다.

이전 단원에서 지정한 사전 조건에 더하여 기본 AMI가 다음 조건을 충족해야 합니다.

- Linux AMI를 사용하려면 `Wget` 또는 `cURL`이 설치 및 구성되어 있어야 합니다. Windows AMI를 사용하려면 PowerShell이 설치되어 있어야 합니다.
- Linux AMI는 EC2 사용자 데이터 스크립트를 실행할 수 있거나, AWS Systems Manager 에이전트(SSM 에이전트)가 미리 설치되어 있어야 합니다.
- Windows AMI를 사용하려면 SSM 에이전트가 미리 설치되어 있어야 합니다.

프라이빗 이미지를 빌드하는 방법

1. AWS Marketplace의 제품 세부 정보 페이지에서 계속 구독하기를 선택합니다.
2. Subscribe to this software(이 소프트웨어 구독) 페이지의 Terms and Conditions(약관 및 조건) 아래에서 세부 정보 표시를 선택하여 제품 인스턴스 유형, 소프트웨어 사용 요금 및 최종 사용자 라이선스 계약(EULA)을 확인합니다. 제품에 따라 여러 가지 유형의 구독이 표시될 수 있습니다. 구독 유형을 선택했으면 약관에 동의를 선택합니다.
3. Continue to Configuration(구성 계속)을 선택합니다.
4. Configure this software(이 소프트웨어 구성) 페이지의 Fulfillment Option(실행 옵션)에서 Private Amazon Machine Image(프라이빗 Amazon 머신 이미지)를 선택합니다.
5. 프라이빗 이미지 섹션의 1. 리전 선택에서 리전을 선택합니다. 2. 시작할 프라이빗 이미지 선택에서 새 프라이빗 이미지 생성을 선택합니다.
6. Create New Private Image(새 프라이빗 이미지 생성) 섹션의 Select a base AMI to use(사용할 기본 AMI 선택)에서 내 소유, 퍼블릭 이미지 또는 프라이빗 이미지를 선택합니다.
   a. 내 소유 – AWS 계정 소유의 AMI
   b. 퍼블릭 이미지 – 모든 AWS 계정이 함께 공유하는 AMI
   c. 프라이빗 이미지 – AWS 계정과 공유하는 AMI
7. 퍼블릭 기본 AMI ID 입력 또는 프라이빗 기본 AMI ID 입력에서 AMI ID를 입력하거나, 혹은 Amazon EC2 콘솔을 사용해 기본 AMI로 사용할 이미지의 AMI ID를 복사하여 붙여넣습니다.
8. Instance Profile(인스턴스 프로파일)에서 사전 필수 단계로서 생성한 인스턴스 역할을 선택합니다.
9. Automation Role(자동화 역할)에서 사전 필수 단계로서 생성한 자동화 역할을 선택합니다.
10. 빌드 로그에 로그를 저장할 Amazon S3 버킷의 이름을 입력합니다. 전체 DNS 이름이 아닌 간단한 버킷 이름(예: *DOC-EXAMPLE-BUCKET*)을 입력합니다.
11. Private Image Name(프라이빗 이미지 이름)에 새로운 프라이빗 이미지 이름을 입력합니다.

새로 생성하는 프라이빗 이미지의 이름을 지정할 때 이미지를 쉽게 식별할 수 있는 이름 지정 규칙을 사용하는 것이 좋습니다. 또한 AWS Marketplace 이미지 빌드 서비스는 새 프라이빗 이미지를 생성할 때 AWSMarketplaceFulfillmentID 태그를 추가하므로, 나중에 프라이빗 이미지를 식별할 때 유용합니다. 그 밖에 다음 옵션 단계에 따라 세부 정보를 추가로 입력하거나, 그렇지 않으면 빌드 시작을 선택하여 빌드 프로세스를 시작할 수도 있습니다.

(선택 사항) 프라이빗 이미지에 대한 세부 정보를 추가로 입력하는 방법

1. 설명 메모에 프라이빗 이미지를 빌드할 때 사용할 인스턴스에 대해 추가하고 싶은 관련 정보를 입력합니다.

2. 인스턴스 유형에서 프라이빗 이미지를 빌드할 때 사용할 인스턴스 유형을 선택합니다.
3. VPC에서 프라이빗 이미지를 빌드할 때 인스턴스가 사용할 VPC를 선택한 다음 보안 그룹과 서브넷을 차례로 선택합니다.
4. Enable Simple Notification System(Simple Notification System 활성화)에서 빌드 상태 변경 시 알림 메시지를 수신할 기존 또는 새로운 주제를 선택합니다.
5. 빌드 시작을 선택합니다.

빌드 프로세스는 완료하는 데 약 1~2시간 걸립니다. 다음은 프로세스와 관련하여 주의해야 할 정보입니다.

- 빌드 프로세스에서 사용되는 서비스 요금은 프라이빗 이미지 빌드 프로세스를 시작할 때 사용한 AWS 계정에 표시됩니다. 여기에는 AWS Marketplace 제품을 프라이빗 이미지에 설치할 때 실행되는 인스턴스와 로그 저장에 사용되는 S3 버킷도 함께 표시됩니다.
- 빌드 프로세스 상태를 확인하거나 Amazon Simple Notification Service(SNS) 메시지를 수신할 수 있습니다.
- 빌드가 완료되면 새 프라이빗 이미지가 AWS 계정에 추가되고 Amazon EC2 콘솔의 내 소유 아래에 사용 가능한 AMI로 표시됩니다.
- 빌드 프로세스를 마칠 때 사용되는 리포지토리는 로컬이어야 합니다.
- 빌드 프로세스 중에는 인터넷 액세스가 차단됩니다.

AMI 별칭 사용

Amazon Machine Image(AMI)는 `AMI ID`로 식별됩니다. `AMI ID`를 사용하여 제품을 시작할 때 사용할 AMI를 지정할 수 있습니다. `AMI ID`의 형식은 `ami-<identifier>`(예: ami-123example456)입니다. 각 AWS 리전의 제품 버전마다 AMI(및 `AMI ID`)가 다릅니다.

AWS Marketplace에서 제품을 시작하면 `AMI ID`가 자동으로 입력됩니다. AWS Command Line Interface(AWS CLI)에서 또는 Amazon Elastic Compute Cloud(Amazon EC2)를 사용하여 자동으로 제품을 시작하려는 경우 `AMI ID`가 있으면 유용합니다. 시작 시 소프트웨어를 구성할 때 `AMI ID`를 찾을 수 있습니다. 자세한 내용은 3단계: 소프트웨어 구성 섹션을 참조하세요.

또한 소프트웨어를 구성할 때 `Ami Alias`는 `AMI ID`와 같은 위치에 있습니다. `Ami Alias`는 `AMI ID`와 비슷한 ID이지만 자동화에 더 편하게 사용할 수 있습니다. `AMI alias`는 `aws/service/marketplace/prod-<identifier>/<version>` 형식(예: `aws/service/marketplace/prod-1234example5678/12.2`)입니다. 이 `Ami Alias` ID는 모든 리전에서 사용할 수 있으며, AWS는 자동으로 이 ID를 올바른 리전 `AMI ID`에 매핑합니다.

최신 버전의 제품을 사용하려면 AMI alias에서 버전 대신 **latest**라는 용어를 사용해야 합니다. 그러면 AWS가 자동으로 최신 버전의 제품을 선택합니다(예: **aws/service/marketplace/prod-1234example5678/latest**).

> **Warning**
>
> 이 **latest** 옵션을 사용하면 가장 최근에 출시된 버전의 소프트웨어가 제공됩니다. 하지만 이 기능은 주의해서 사용해야 합니다. 예를 들어 제품 버전으로 1.x 버전과 2.x 버전이 있으면 아마도 2.x 버전을 선택할 것입니다. 하지만 1.x의 버그 픽스가 가장 최근에 출시된 제품 버전일 수도 있습니다.

AMI 별칭 사용 예제

AMI 별칭은 자동화에 유용합니다. AWS CLI 또는 AWS CloudFormation 템플릿에서 AMI 별칭을 사용할 수 있습니다.

다음은 AWS CLI에서 AMI 별칭을 사용하여 인스턴스를 시작하는 방법을 보여주는 예제입니다.

```
aws ec2 run-instances
--image-id resolve:ssm:/aws/service/marketplace/<identifier>/version-7.1
--instance-type m5.xlarge
--key-name MyKeyPair
```

다음은 AMI 별칭을 입력 파라미터로 수락하여 인스턴스를 생성하는 CloudFormation 템플릿을 보여주는 예제입니다.

```
AWSTemplateFormatVersion: 2010-09-09

Parameters:
    AmiAlias:
        Description: AMI alias
        Type: 'String'

Resources:
    MyEC2Instance:
        Type: AWS::EC2::Instance
        Properties:
            ImageId: !Sub "resolve:ssm:${AmiAlias}"
            InstanceType: "g4dn.xlarge"
            Tags:
```

```
                -Key: "Created from"
                 Value: !Ref AmiAlias
```

컨테이너 제품

컨테이너 제품은 컨테이너 이미지로 처리되는 독립형 제품입니다. 컨테이너 제품은 무료일 수도 있고 판매자가 제시하는 가격 옵션에 따라 비용을 지불해야 할 수도 있습니다. 컨테이너 제품은 Amazon Elastic Container Service(Amazon ECS), Amazon Elastic Kubernetes Service(Amazon EKS), 고객의 자체 인프라에서 실행되는 서비스를 비롯한 여러 컨테이너 런타임 및 서비스와 함께 사용할 수 있습니다. 지원되는 런타임 및 서비스의 전체 목록과 각각에 대한 자세한 내용은 컨테이너 제품에 지원되는 서비스에서 확인할 수 있습니다.

AWS Marketplace 웹 사이트 또는 Amazon ECS 콘솔에서 컨테이너 제품을 검색, 구독 및 배포할 수 있습니다. 판매자가 제공하는 작업 정의, Helm 등의 배포 템플릿을 사용하여 Amazon ECS 또는 Amazon EKS에 여러 제품을 배포할 수 있습니다. 또는 해당 제품을 구독한 후 프라이빗 Amazon Elastic Container Registry(Amazon ECR) 리포지토리에서 직접 컨테이너 이미지에 액세스할 수 있습니다.

제품에서 QuickLaunch를 지원하는 경우 QuickLaunch를 사용하여 Amazon EKS 클러스터에서 불과 몇 단계 만에 신속하게 컨테이너 제품을 테스트할 수 있습니다. QuickLaunch는 AWS CloudFormation을 사용하여 Amazon EKS 클러스터를 생성하고 해당 클러스터에서 컨테이너를 시작합니다. QuickLaunch에서 시작하는 방법에 대한 자세한 내용은 AWS Marketplace의 QuickLaunch 섹션을 참조하세요.

이 섹션에서는 AWS Marketplace에서 컨테이너 제품을 검색, 구독 및 시작하는 방법에 대한 정보를 제공합니다.

유료 컨테이너 제품에 적용되는 요금 모델

유료 컨테이너 제품에는 하나 이상의 요금 모델이 있어야 합니다. AWS Marketplace의 다른 유료 제품과 마찬가지로 AWS에서는 유료 컨테이너 제품에 대해서도 요금 모델에 따라 요금을 청구합니다. 요금 모델은 월 정액제 또는 초 단위로 모니터링하여 비례 배분 방식으로 계산하는 시간당 요금제입니다. 자세한 요금 정보는 세부 정보 페이지에 나와 있으며 제품을 구독할 때 제공됩니다.

AWS Marketplace의 컨테이너 제품이 지원하는 요금 모델은 다음과 같습니다.

- 무제한으로 사용할 수 있는 월 정액제
- 장기 계약 기간 동안 제품을 사용할 수 있는 선결제
- 제품 사용량에 따른(일반적으로 시간당) 사용한 만큼만 지불

- 계약 요금이 적용되는 선결제 모델

각 모델에 대한 자세한 내용은 AWS Marketplace판매자 가이드의 컨테이너 제품 요금을 참조하세요.

컨테이너 및 Kubernetes 개요

Docker 컨테이너와 같은 컨테이너는 Linux나 Windows Server 같은 가상화 운영 체제에 추상화 및 자동화 계층을 추가하는 오픈 소스 소프트웨어 기술입니다. 가상 머신이 서버 이미지 인스턴스인 것처럼 컨테이너 역시 도커 컨테이너 이미지 인스턴스입니다. 도커 컨테이너는 실행하는 데 필요한 모든 것, 즉 코드, 런타임, 시스템 도구, 시스템 라이브러리 등이 포함된 파일 시스템에서 서버 애플리케이션 소프트웨어를 래핑합니다. 컨테이너를 사용하면 환경에 관계없이 소프트웨어가 항상 동일하게 실행됩니다.

컨테이너는 Java 가상 머신과 비슷하여 운영 체제에서, 그리고 서로 격리되는 동시에 변환 및 오케스트레이션 계층을 제공할 기본 플랫폼이 필요합니다. Docker 컨테이너와 함께 사용할 수 있는 다양한 도커 호환 런타임 및 오케스트레이션 서비스가 있으며, 여기에는 AWS를 위한 확장성이 뛰어난 고성능 오케스트레이션 서비스인 Amazon ECS와 오픈 소스 관리 및 오케스트레이션 서비스인 Kubernetes를 사용하여 컨테이너화된 애플리케이션을 쉽게 배포, 관리 및 확장할 수 있는 Amazon EKS가 포함됩니다.

컨테이너 제품 찾기 및 구독

컨테이너 제품은 컨테이너 이미지로 시작할 수 있는 AWS Marketplace의 제품입니다. 판매자가 컨테이너 이미지, 차트 Helm 또는 아마존 EKS 추가 기능 제공 방법을 통해 이행 옵션을 제공한 AWS Marketplace의 모든 상품이 컨테이너 제품에 포함됩니다. 컨테이너 제품 제공 방법에 대한 자세한 내용은 컨테이너 제품 제공 방법 섹션을 참조하세요.

지원되는 서비스라고도 하는 여러 시작 환경을 컨테이너 제품의 이행 옵션으로 사용할 수 있습니다. 시작 환경으로는 Amazon Elastic Container Service(Amazon ECS), Amazon Elastic Kubernetes Service(Amazon EKS), 자체 관리형 인프라 등의 서비스가 있습니다. 사용 가능한 컨테이너 제품 시작 환경의 전체 목록은 컨테이너 제품에 지원되는 서비스 섹션을 참조하세요.

AWS Marketplace 웹 사이트를 사용하여 컨테이너 제품 검색

AWS Marketplace 웹 사이트를 사용하여 컨테이너 제품을 검색할 수 있습니다.

AWS Marketplace 웹 사이트를 사용하여 컨테이너 제품을 검색하는 방법

1. AWS Marketplace 검색 페이지로 이동합니다.

2. 제공 방법을 컨테이너 이미지 또는 차트 Helm으로 필터링합니다.
3. (선택 사항) 지원되는 서비스를 필터링하면 제품을 시작할 수 있는 서비스로 검색 결과를 좁힐 수 있습니다.

원하는 제품을 찾은 후에는 제목을 선택하여 제품 세부 정보 페이지로 이동합니다.

컨테이너 제품 세부 정보 페이지

AWS Marketplace의 제품 세부 정보 페이지에서 다음 정보를 포함하여 제품에 대한 세부 정보를 찾을 수 있습니다.

- 제품 개요 - 개요에는 제품 설명과 다음 정보가 포함되어 있습니다.
  - 보고 있는 제품 버전.
  - 판매자의 프로필 링크.
  - 이 제품이 속한 제품 범주.
  - 이 소프트웨어를 실행할 수 있는 운영 체제.
  - 소프트웨어를 시작하는 데 사용할 수 있는 제공 방법.
  - 이 제품을 시작할 수 있는 서비스.
- 요금 정보 - 프리 티어, 기존 보유 라이선스 사용(BYOL), 계약 요금이 적용되는 선결제, 월간 또는 연간 고정 가격이나 시간당 요금이 부과되는 사용한 만큼만 지불 등이 있습니다. 요금 모델에 대한 자세한 내용은 컨테이너 제품 요금을 참조하세요.
- 사용 정보 - 여기에는 판매자가 제공하는 이행 옵션과 소프트웨어를 시작하고 실행하는 방법에 대한 지침이 포함되어 있습니다. 각 상품에는 이행 옵션이 하나 이상 있어야 하며 최대 5개까지 가능합니다. 각 이행 옵션에는 제공 방법과 소프트웨어를 시작하고 실행할 때 따라야 하는 지침이 포함되어 있습니다.
- 지원 정보 - 이 섹션에는 제품에 대한 지원을 받는 방법과 환불 정책에 대한 세부 정보가 포함되어 있습니다.
- 고객 리뷰 - 다른 고객의 제품 리뷰를 찾거나 직접 리뷰를 작성할 수 있습니다.

제품을 구독하려면 제품 세부 정보 페이지에서 계속 구독하기를 선택합니다. 제품 구독에 대한 자세한 내용은 AWS Marketplace의 제품 구독 섹션을 참조하세요.

AWS Marketplace의 제품 구독

제품을 사용하려면 먼저 제품을 구독해야 합니다. 구독 페이지에서 유료 제품의 요금 정보를 확인하고 소프트웨어 최종 사용자 라이선스 계약(EULA)에 액세스할 수 있습니다.

컨테이너 계약 요금이 적용되는 제품의 경우 계약 요금을 선택하고 계약 수락을 선택하여 계속 진행합니다. 그러면 제품 구독이 생성되고, 소프트웨어 사용 권한이 부여됩니다. 구독이 완료될 때까지 1~2분 정도 걸립니다. 유료 제품에 대한 권한이 부여되면 소프트웨어를 사용하는 순간부터 요금이 청구됩니다. 실행 중인 소프트웨어 인스턴스를 모두 종료하지 않고 구독을 취소할 경우 소프트웨어 사용량에 대한 요금이 계속해서 청구됩니다. 제품 사용과 관련하여 인프라 요금이 발생할 수도 있습니다. 예를 들어 소프트웨어 제품을 호스팅할 목적으로 새로운 Amazon EKS 클러스터를 생성하면 해당 서비스에 대한 요금이 청구됩니다.

> **Note**
>
> 컨테이너 기반 제품을 구독하고 배포하는 방법에 대한 자세한 내용은 다음 비디오를 참조하세요.
>
> - Amazon ECS 클러스터에 AWS Marketplace 컨테이너 배포(3:34)
> - Amazon ECS Anywhere를 사용하여 AWS Marketplace 컨테이너 기반 제품 배포(5:07)
> - Amazon EKS 추가 기능 관리

컨테이너 제품 제공 방법

판매자가 컨테이너 이미지, 차트 Helm 또는 Amazon EKS 추가 기능 제공 방법을 통해 하나 이상의 이행 옵션을 제공하는 경우 AWS Marketplace의 모든 상품이 컨테이너 제품으로 간주됩니다.

컨테이너 이미지 제공 방법

컨테이너 이미지 제공 방법을 사용하는 이행 옵션의 경우 판매자가 제공한 지침에 따라 제품을 시작합니다. 이 작업은 Amazon Elastic 컨테이너 레지스트리의 AWS Marketplace 레지스트리에서 직접 도커 이미지를 가져오는 방식으로 이루어집니다. 이 제공 방법으로 시작하는 방법에 대한 자세한 내용은 컨테이너 이미지 이행 옵션으로 시작 섹션을 참조하세요.

차트 Helm 제공 방법

차트 Helm 제공 방법을 사용하는 이행 옵션의 경우 판매자가 제공한 지침 또는 배포 템플릿을 사용하여 제품을 시작합니다. 이 작업은 Helm CLI를 사용하여 차트 Helm을 설치하는 방식으로 이루어집니다. 기존 Amazon EKS 클러스터, EKS Anywhere의 자체 관리형 클러스터, Amazon Elastic Compute Cloud(Amazon EC2) 또는 온프레미스에서 애플리케이션을 시작할 수 있습니다. 이 제공 방법으로 시작하는 방법에 대한 자세한 내용은 Helm 이행 옵션으로 시작 섹션을 참조하세요.

Amazon EKS 추가 기능의 제공 방법

Amazon EKS 추가 기능 제공 방법을 사용하는 이행 옵션의 경우 Amazon EKS 콘솔 또는 Amazon EKS CLI를 사용하여 제품을 시작합니다. Amazon EKS 추가 기능에 대한 자세한 내용은 Amazon EKS 추가 기능을 참조하세요.

컨테이너 제품에 지원되는 서비스

다음 목록에는 AWS Marketplace의 컨테이너 제품에 지원되는 모든 서비스가 포함되어 있습니다. 지원되는 서비스는 제품을 시작할 수 있는 컨테이너 서비스 또는 환경입니다. 컨테이너 제품은 제공 방법과 하나 이상의 환경에서 시작하기 위한 지침이 포함된 이행 옵션을 하나 이상 포함하고 있어야 합니다.

Amazon ECS

Amazon Elastic Container Service(Amazon ECS)는 클러스터에서 컨테이너를 실행, 중지 및 관리할 수 있는 컨테이너 관리 서비스로써 확장성과 속도가 뛰어납니다. 컨테이너는 서비스 내에서 개별 태스크나 여러 태스크를 실행하는 데 사용하는 태스크 정의에 정의됩니다. 이러한 맥락에서 서비스는 지정된 수의 작업을 클러스터에서 동시에 실행하고 유지 관리할 수 있는 구성입니다. AWS Fargate에서 관리하는 서버를 사용하지 않는 인프라에서 태스크 및 서비스를 실행할 수 있습니다. 또는 인프라에 대한 더 세부적인 제어를 위해 관리하는 Amazon EC2 인스턴스의 클러스터에서 태스크와 서비스를 실행할 수 있습니다.

Amazon ECS에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 Amazon Elastic Container Service란 무엇입니까?를 참조하세요.

Amazon EKS

Amazon Elastic Kubernetes Service(Amazon EKS)는 Kubernetes를 실행하는 데 사용할 수 있는 관리형 서비스입니다. AWS Kubernetes 제어 플레인 또는 노드를 설치, 작동 및 유지 관리할 필요가 없습니다. Kubernetes는 컨테이너화된 애플리케이션의 배포, 조정 및 관리 자동화를 위한 오픈 소스 시스템입니다.

Amazon EKS 콘솔을 사용하여 타사 Kubernetes 소프트웨어를 검색, 구독 및 배포할 수 있습니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS 추가 기능 관리를 참조하세요.

자체 관리형 Kubernetes

EKS Anywhere, Amazon ECS Anywhere, Amazon EC2 또는 온프레미스 인프라에서 실행되는 자체 관리형 Kubernetes 클러스터에서 컨테이너 제품을 시작할 수 있습니다.

Amazon ECS Anywhere는 고객 관리형 인프라에서 컨테이너 워크로드를 실행하고 관리하는 데 사용할 수 있는 Amazon ECS의 기능입니다. Amazon ECS Anywhere는 Amazon ECS를 기반으로 구축되며 컨테이너 기반 애플리케이션 전반에 걸쳐 일관된 도구 및 API 경험을 제공합니다.

자세한 내용은 Amazon ECS Anywhere를 참조하세요.

EKS Anywhere는 고객 관리형 인프라에서 Amazon EKS 클러스터를 생성하는 데 사용할 수 있는 서비스입니다. EKS Anywhere를 지원되지 않는 로컬 환경으로 또는 지원되는 온프레미스 Kubernetes 플랫폼이 될 수 있는 프로덕션 품질 환경으로 배포할 수 있습니다.

EKS Anywhere에 대한 자세한 내용은 EKS Anywhere 설명서를 참조하세요.

Amazon ECS 콘솔을 사용하여 컨테이너 제품 검색

컨테이너 제품은 Amazon ECS 콘솔에서도 찾을 수 있습니다. AWS Marketplace에서 신제품을 검색하고 기존 구독을 볼 수 있는 링크가 탐색 창에 있습니다.

구독 취소

제품 구독을 취소하려면 사용자 소프트웨어 페이지를 사용하십시오.

계약 요금이 적용되는 컨테이너 제품

일부 판매자는 계약 요금 모델이 적용되는 공개 컨테이너 기반 소프트웨어 제품을 제공합니다. 계약 요금 모델은 개별 수량의 라이선스를 선불로 한 번 결제하는 데 동의하면 구매자가 선택한 기간 동안 소프트웨어 제품에 액세스할 수 있는 모델이며, 요금은 AWS 계정를 통해 선불로 청구됩니다.

Example 다양한 유형의 라이선스를 다양한 수량으로 구매

예를 들어 사용자 액세스 라이선스 10개와 관리 라이선스 5개 1년 사용권을 구매할 수 있습니다. 라이선스를 자동으로 갱신하도록 선택할 수 있습니다.

또한 일부 회사는 계약 요금 모델이 적용되는 비공개 컨테이너 기반 소프트웨어 제품을 제공합니다. 비공개 제안은 일반적으로 기간이 고정되어 있으며 기간을 변경할 수 없습니다.

AWS Marketplace의 제품 세부 정보 페이지에서 컨테이너 기반 소프트웨어 제품 계약을 구매할 수 있습니다. 이 옵션을 사용할 수 있으면 제품 세부 정보 페이지에서 제공 방법으로 계약 요금이 적용되는 AMI가 표시됩니다. 제품을 구매하면 계정 설정 및 구성을 위해 해당 제품의 웹 사이트로 이동됩니다. 이후부터는 정기 AWS 계정 청구서에 사용 요금이 표시됩니다.

AWS Marketplace의 계약 요금 공개 제안이 적용되는 컨테이너 제품 구독

계약 요금 모델이 적용되는 공개 제안 컨테이너 기반 제품을 구독하는 방법

> **Note**
>
> Amazon EKS를 사용한 구독에 대한 자세한 내용은 Amazon EKS 추가 기능 관리를 참조하세요.

1. AWS Marketplace에 로그인하고 계약 요금 모델이 적용되는 컨테이너 기반 소프트웨어 제품을 찾습니다.
2. 조달 페이지에서 요금 정보를 확인합니다.

   단위와 각 기간(개월 단위)의 요율을 확인할 수 있습니다.
3. 구독을 시작하려면 계속 구독하기를 선택합니다.

   구독하지 않고 이 제품을 저장하려면 목록에 저장을 선택합니다.
4. 요금 정보를 검토하고 소프트웨어 제품 조건을 구성하여 계약을 생성합니다.

   a. 계약 기간을 1개월, 12개월, 24개월 또는 36개월 중에 선택합니다.

   b. 갱신 설정에서 계약 자동 갱신 여부를 선택합니다.

   c. 계약 옵션에서 각 단위의 수량을 선택합니다.

   총 계약 요금은 요금 세부 정보에 표시됩니다.
5. 선택을 마쳤으면 계약 생성을 선택합니다.

총 계약 요금이 구매자의 AWS 계정에 청구되며 라이선스는 AWS License Manager에 생성됩니다.

> **Note**
>
> 구독이 처리되고 License Manager 계정에 소프트웨어 제품의 라이선스가 생성될 때까지 최대 10분이 걸릴 수 있습니다.

AWS Marketplace의 계약 요금 비공개 제안이 적용되는 컨테이너 제품 구독

계약 요금 모델이 적용되는 비공개 제안 컨테이너 기반 제품을 구독하는 방법

> **Note**
>
> Amazon EKS를 사용한 구독에 대한 자세한 내용은 Amazon EKS 추가 기능 관리를 참조하세요.

1. 구매자 계정으로 AWS Marketplace에 로그인합니다.
2. 비공개 제안을 봅니다.
3. 조달 페이지에서 요금 정보를 확인합니다.

   단위와 각 기간(개월 단위)의 요율을 확인할 수 있습니다.
4. 계속 구독하기를 선택하여 구독을 시작합니다.
5. 요금 정보를 검토하고 소프트웨어 제품 조건을 구성하여 계약을 생성합니다.

   계약 기간은 판매자가 이미 설정했으며 수정할 수 없습니다.
6. 계약 옵션에서 각 단위의 수량을 선택합니다.
7. 요금 세부 정보에서 총 계약 요금을 확인합니다.

   사용 가능한 다른 제안에서 혜택 보기를 선택하여 공개 제안을 볼 수도 있습니다.
8. 선택을 마쳤으면 계약 생성을 선택합니다.

> **Note**
>
> 구독이 처리되고 License Manager 계정에 소프트웨어 제품의 라이선스가 생성될 때까지 최대 10분이 걸릴 수 있습니다.

소프트웨어 액세스

컨테이너 기반 소프트웨어 제품에 액세스하는 방법

1. AWS Marketplace 콘솔에서 구독 보기로 이동하여 소프트웨어 제품의 라이선스를 확인합니다.
2. 조달 페이지에서 다음을 수행합니다.

a. 라이선스 관리를 선택하여 AWS License Manager에서 사용 권한을 보고, 액세스 권한을 부여하고, 사용 현황을 추적합니다.

b. Continue to Configuration(구성 계속)을 선택합니다.

3. 시작 페이지에서 컨테이너 이미지 세부 정보를 확인하고 표시되는 지침을 따릅니다.

Amazon Elastic Container Service(Amazon ECS) 클러스터를 생성할 때 IAM 정책에 다음 AWS Identity and Access Management(IAM) 권한을 추가해야 합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "license-manager:CheckoutLicense",
            "license-manager:GetLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:ListReceivedLicenses"
         ],
         "Resource":"*"
      }
   ]
}
```

생성된 라이선스 확인

생성된 라이선스를 확인하는 방법

1. AWS 계정로 AWS License Manager에 로그인합니다.
2. 권한 부여된 라이선스에서 권한 부여된 모든 라이선스를 확인합니다.
3. 검색 창에 제품 SKU, 수신자 또는 상태를 입력하여 라이선스를 검색합니다.
4. 라이선스 ID를 선택하고 라이선스 세부 정보를 확인합니다.
5. 발행자(AWS/Marketplace) 및 권한(라이선스가 애플리케이션 또는 리소스를 사용, 액세스 또는 소비할 수 있는 권한을 부여하는 단위)을 볼 수 있습니다.

기존 계약 수정

컨테이너 제품에 대한 기존 선결제 약정이 있는 경우 AWS Marketplace 구매자는 계약의 일부 조항을 수정할 수 있습니다. 컨테이너 계약은 시간당 또는 연간 유연한 소비 요금(FCP) 제안과 달리 계약 조건 기반 제안을 통해 지원됩니다. 이 기능은 AWS License Manager와 통합된 애플리케이션에서만 사용할 수 있습니다. 구매자는 현재 계약에서 동일한 제안의 권한 내에서 추가 라이선스를 구매할 수 있습니다. 하지만 구매자는 계약에서 구매한 권한 수를 줄일 수 없습니다. 또한 판매자가 자동 구독 갱신 옵션을 활성화한 경우 구매자는 자동 구독 갱신을 취소할 수 있습니다.

> **Note**
>
> 유연한 결제 일정(FPS) 계약 제안은 수정할 수 없습니다. FPS 구매 계약에 대해서는 구매자가 변경할 수 있는 권한이 없습니다. 권한은 애플리케이션 또는 리소스를 사용, 액세스 또는 소비할 수 있는 권리입니다. FPS 제안은 변경할 수 없습니다.

구독 관리

1. AWS Marketplace 콘솔에서 구독 보기로 이동하여 소프트웨어 제품의 라이선스를 확인합니다.
2. 조달 페이지에서 라이선스 관리를 선택합니다.
3. 목록에서 약관 보기를 선택합니다.
4. 계약 옵션 섹션에서 화살표를 사용하여 권한을 늘립니다. 권한 개수를 구매한 권한 아래로 줄일 수 없습니다.
5. 계약 세부 정보 및 총 가격은 요금 세부 정보 섹션에 표시됩니다.

자동 구독 갱신을 취소하는 방법

1. AWS Marketplace 콘솔에서 구독 보기로 이동하여 소프트웨어 제품의 라이선스를 확인합니다.
2. 조달 페이지에서 라이선스 관리를 선택합니다.
3. 구독 페이지에서 갱신 설정 섹션을 찾습니다.
4. 취소와 관련된 이용 약관을 이해합니다.
5. 확인란을 선택하여 자동 갱신 옵션을 취소합니다.

AWS Marketplace에서 컨테이너 소프트웨어 시작

AWS Marketplace에서 컨테이너 제품의 구독을 활성화한 후에는 소프트웨어를 시작해야 합니다. 소프트웨어를 시작하려면 판매자가 제공한 이행 옵션 중 하나에 포함된 지침을 따릅니다. AWS Marketplace에서 이행 옵션은 구매자의 환경에서 제품을 시작할 수 있도록 판매자가 제공하는 선택적 절차입니다. 컨테이너 제품의 경우 판매자는 최대 네 가지 이행 옵션을 제공할 수 있으며, 각 옵션은 서로 다른 제공 방법을 사용하고 서로 다른 소프트웨어 구성을 제시할 수 있습니다. 예를 들어 판매자는 제품 테스트에 사용되는 이행 옵션을 하나 생성하고, 기업 내에서 대규모로 배포하는 데 사용되는 다른 이행 옵션을 생성할 수 있습니다.

AWS Marketplace에서 제품 세부 정보 페이지의 사용 정보 섹션을 보면 어떤 이행 옵션을 사용할 수 있는지 확인할 수 있습니다. 각 이행 옵션은 지원되는 서비스에 대한 정보를 포함하고 있으며 소프트웨어 버전 세부 정보를 제공합니다. Amazon Elastic Container Service(Amazon ECS) 및 Amazon Elastic Kubernetes Service(Amazon EKS)를 예로 들 수 있습니다. 사용 지침을 선택하면 웹 서버에 로그인하는 방법, 시작 후 구성 등과 같은 제품 사용 방법에 대한 판매자의 설명서를 볼 수 있습니다.

> **Note**
>
> 컨테이너 기반 제품을 구독하고 배포하는 방법에 대한 자세한 내용은 다음 비디오를 참조하세요.
>
> - Amazon ECS 클러스터에 AWS Marketplace 컨테이너 배포(3:34)
> - Amazon ECS Anywhere를 사용하여 AWS Marketplace 컨테이너 기반 제품 배포(5:07)

ECS Anywhere를 사용하여 AWS Marketplace 컨테이너 기반 제품 배포

AWS Marketplace에서 컨테이너 소프트웨어 시작

AWS Marketplace에서 컨테이너 소프트웨어를 시작하는 방법

1. AWS Marketplace에 로그인합니다.
2. AWS Marketplace를 찾은 다음, 시작하려는 소프트웨어가 포함된 제품을 찾습니다. 소프트웨어를 시작하려면 제품을 구독해야 합니다. AWS Marketplace에서 컨테이너 제품을 검색하고 구독하는 방법에 대한 자세한 내용은 컨테이너 제품 찾기 및 구독 섹션을 참조하세요.
3. 제품 세부 정보 페이지에서 계속 구독하기를 선택합니다.
4. Continue to Configuration(구성 계속)을 선택합니다. 이 버튼이 보이지 않으면 약관에 동의하지 않았거나 제품을 구독하지 않은 것일 수 있습니다.

5. 이행 옵션에서, 판매자가 제공한 옵션 목록 중에 이행 옵션을 선택합니다. 이행 옵션을 선택하면 지원되는 서비스에서 시작할 수 있는 서비스를 볼 수 있습니다. 이행 옵션에 대한 자세한 내용은 컨테이너 제품 이행 옵션 섹션을 참조하세요.
6. 계속해서 시작을 선택합니다.
7. 판매자가 제공한 지침에 따라 제품을 시작합니다. 지침은 이행 옵션에 따라 다릅니다. 자세한 내용은 컨테이너 이미지 이행 옵션으로 시작 또는 Helm 이행 옵션으로 시작 섹션을 참조하세요.
8. 선택 사항 - 제품을 시작한 후 구성하고 사용하는 방법에 대한 판매자의 설명서를 보려면 사용 지침을 선택합니다.

컨테이너 제품 이행 옵션

제품 세부 정보 페이지의 사용 정보 섹션을 보면 어떤 이행 옵션을 사용할 수 있는지 확인할 수 있습니다. AWS Marketplace에는 판매자가 제공하는 이행 옵션 외에도 Amazon Elastic Container Registry(Amazon ECR)에서 직접 도커 이미지를 가져오는 방법에 대한 지침이 포함되어 있습니다.

이행 옵션은 판매자가가 제공하므로 이행 옵션의 이름과 내용은 AWS Marketplace의 제품마다 다릅니다. 상품과 판매자마다 방법이 다르지만, 각 이행 옵션에는 제공 방법이 포함되어야 합니다. 제공 방법을 이행 옵션 유형이라고 생각하면 됩니다. 컨테이너 상품에 사용할 수 있는 세 가지 제공 방법은 컨테이너 이미지, 차트 Helm 및 Amazon EKS 추가 기능입니다.

컨테이너 이미지 이행 옵션으로 시작

컨테이너 이미지 제공 방법을 사용하는 이행 옵션의 경우 판매자가 제공한 지침에 따라 제품을 시작합니다. 이 작업은 Amazon ECR에서 직접 도커 이미지를 가져오는 방식으로 이루어집니다. 제품을 시작하는 일반적인 단계는 다음과 같습니다.

1. 최신 버전의 AWS Command Line Interface(AWS CLI) 및 Docker가 설치되어 있는지 확인합니다. 자세한 정보는 Amazon Elastic Container Registry 사용 설명서의 AWS CLI에서 Amazon ECR 사용을 참조하세요.
2. Docker 클라이언트를 Amazon ECR 레지스트리에 인증합니다. 이 작업을 수행하는 단계는 운영 체제에 따라 다릅니다.
3. 제공된 Amazon ECR 이미지 Amazon 리소스 이름(ARN)을 사용하여 모든 도커 이미지를 가져옵니다. 자세한 내용은 Amazon Elastic Container Registry 사용 설명서의 이미지 가져오기기를 참조하세요.
4. 제품 사용에 대한 내용은 판매자가 제공한 사용 지침이나 외부 링크를 검토하세요.

Helm 이행 옵션으로 시작

Helm 제공 방법을 사용하는 이행 옵션의 경우 판매자가 제공한 지침에 따라 제품을 시작합니다. 이 작업은 Helm CLI를 사용하여 차트 Helm을 설치하는 방식으로 이루어집니다. 기존 Amazon EKS 클러스터, EKS Anywhere의 자체 관리형 클러스터, Amazon Elastic Compute Cloud(Amazon EC2) 또는 온프레미스에서 애플리케이션을 시작할 수 있습니다.

> **Note**
>
> 시작 환경은 Helm CLI 버전 3.7.1을 사용해야 합니다. Helm 버전 목록은 GitHub의 Helm 릴리스를 참조하세요.

판매자가 QuickLaunch를 활성화한 경우 QuickLaunch를 사용하여 애플리케이션을 시작할 수 있습니다. QuickLaunch는 AWS CloudFormation을 사용하여 Amazon EKS 클러스터를 생성하고 해당 클러스터에서 애플리케이션을 시작하는 AWS Marketplace의 기능입니다. QuickLaunch에 대한 자세한 내용은 AWS Marketplace의 QuickLaunch 섹션을 참조하세요.

지침은 판매자가 제공하며 판매자와 제품마다 다릅니다. Helm 이행 옵션으로 제품을 시작하는 일반적인 단계는 다음과 같습니다.

Helm 이행 옵션으로 제품을 시작하는 방법

1. AWS Marketplace에서 컨테이너 소프트웨어 시작의 1~6단계를 따르고, 차트 Helm 제공 방법이 포함된 이행 옵션을 선택합니다.
2. 시작 대상에서 배포 환경을 선택합니다.
   - Amazon EKS에서 애플리케이션을 배포하려면 Amazon 관리형 Kubernetes를 선택합니다. 판매자가 QuickLaunch를 활성화한 경우 QuickLaunch를 사용하여 새 Amazon EKS 클러스터를 생성하고 해당 클러스터에서 애플리케이션을 실행할 수 있습니다.
   - EKS Anywhere에 애플리케이션을 배포하거나 Amazon EC2 또는 온프레미스에서 실행되는 Kubernetes 클러스터에 애플리케이션을 배포하려면 자체 관리형 Kubernetes를 선택합니다.
3. Amazon 관리형 Kubernetes 클러스터에서 시작하는 경우:
   a. Amazon EKS의 기존 클러스터에서 시작하려면 시작 방법에서 기존 클러스터에서 시작을 선택하고 시작 지침을 따릅니다. 이 지침에는 AWS Identity and Access Management(IAM) 역할을 생성하고 애플리케이션을 시작하는 내용이 포함되어 있습니다. Helm CLI 버전 3.7.1을 사용하고 있는지 확인합니다.

b. QuickLaunch를 사용하여 새 Amazon EKS 클러스터를 생성하고 해당 클러스터에서 애플리케이션을 시작하려면 시작 방법에서 QuickLaunch를 사용하여 새 EKS 클러스터에서 시작을 선택합니다. 시작을 선택합니다. 그러면 AWS CloudFormation 콘솔에서 스택을 생성하도록 리디렉션됩니다. 이 스택은 Amazon EKS 클러스터를 생성하고 판매자가 제공한 차트 Helm을 설치하여 애플리케이션을 배포합니다.

c. 빠른 스택 생성 페이지의 스택 이름에 이 스택의 이름을 입력합니다.

d. 파라미터 타일의 정보를 검토하고 필요한 정보를 입력합니다. 기능에서 확인 내용을 검토 및 선택하고 스택 생성을 선택합니다.

> **Note**
>
> AWS CloudFormation, 스택 및 생성된 Amazon EKS 클러스터에 대한 정보를 포함하여 QuickLaunch에 대한 자세한 내용은 AWS Marketplace의 QuickLaunch 섹션을 참조하세요.

4. 자체 관리형 Kubernetes 클러스터에서 시작하는 경우:

a. Helm CLI 버전 3.7.1을 사용하고 있는지 확인합니다.

b. 토큰 생성을 선택하여 라이선스 토큰과 IAM 역할을 생성합니다. 이 토큰과 역할은 제품 사용 권한을 검증하기 위해 AWS License Manager와 통신하는 데 사용됩니다.

> **Note**
>
> 한 계정에 허용되는 최대 라이선스 토큰 수는 10개입니다.

c. 생성된 토큰 정보가 포함된 .csv 파일을 다운로드하려면 CSV로 다운로드를 선택합니다. 모든 보안 암호 및 암호와 마찬가지로 .csv 파일도 안전한 위치에 저장합니다.

d. Kubernetes 보안 암호로 저장의 명령을 실행하여 라이선스 토큰과 IAM 역할을 Kubernetes 클러스터에 보안 암호로 저장합니다. 이 보안 암호는 차트 Helm을 설치하고 애플리케이션을 시작할 때 사용됩니다. AWS Marketplace는 보안 암호를 사용하여 이 제품 사용 권한을 확인합니다.

e. 토큰을 사용하여 애플리케이션 시작의 명령을 실행하여 애플리케이션을 클러스터에 배포하는 차트 Helm을 설치합니다.

f. 제품을 시작한 후 구성하고 사용하는 방법에 대한 판매자의 설명서를 보려면 사용 지침을 선택합니다.

g. 선택 사항 - [선택 사항] 아티팩트 다운로드에 제공된 명령을 사용하여 제품의 컨테이너 이미지와 차트 Helm을 로컬로 다운로드합니다.

Amazon EKS 이행 옵션으로 시작

Amazon EKS 추가 기능 제공 방법을 사용하는 이행 옵션의 경우 Amazon EKS 콘솔을 사용하여 Amazon EKS 클러스터에 소프트웨어를 배포합니다. 제품을 시작하는 일반적인 단계는 다음과 같습니다.

Amazon EKS 이행 옵션으로 제품을 시작하는 방법

1. 제품을 구독한 후, 구성 페이지로 이동하고 Amazon EKS 콘솔 계속하기를 선택하여 Amazon EKS 콘솔에 액세스합니다.
2. Amazon EKS 콘솔에서 클러스터가 배포된 AWS 리전을 선택합니다. 소프트웨어를 배포할 클러스터를 선택합니다.
3. 추가 기능(Add-ons) 탭을 선택합니다.
4. 추가 기능 가져오기를 선택하고, 화면을 스크롤하여 배포하려는 추가 기능을 찾고, 다음을 선택합니다.
5. 배포하려는 버전을 선택하고 다음을 선택합니다. Amazon EKS 배포에 대한 자세한 내용은 EKS 추가 기능을 참조하세요.
6. 선택한 내용을 검토하고 생성을 선택합니다.

AWS Marketplace의 QuickLaunch

판매자가 이행 옵션에서 QuickLaunch를 활성화한 경우 QuickLaunch를 사용하여 Amazon EKS 클러스터를 생성하고 해당 클러스터에 컨테이너 애플리케이션을 배포할 수 있습니다. QuickLaunch를 선택하면 AWS CloudFormation을 사용하여 Amazon EKS 클러스터를 구성 및 생성하고 해당 클러스터에서 컨테이너 애플리케이션을 시작하게 됩니다. QuickLaunch를 사용하면 테스트 목적으로 컨테이너 애플리케이션을 시작할 수 있습니다. QuickLaunch를 사용하려면 Helm 이행 옵션으로 시작의 단계를 따릅니다.

애플리케이션을 배포할 수 있는 Amazon EKS 클러스터를 생성하려면 CloudFormation 스택을 생성합니다. 스택이란 하나의 단위로 관리할 수 있는 AWS 리소스의 모음입니다. 스택의 모든 리소스는 스택의 CloudFormation 템플릿으로 정의합니다. QuickLaunch의 스택 리소스에는 Amazon EKS 클러스터를 생성하고 애플리케이션을 시작하는 데 필요한 정보가 포함되어 있습니다. AWS CloudFormation의 스택에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 스택 작업을 참조하세요.

클러스터가 생성되면 QuickLaunch는 판매자가 제공한 차트 Helm을 클러스터에 설치하여 클러스터에서 애플리케이션을 시작합니다. QuickLaunch는 Amazon EKS 클러스터를 생성하는 스택 생성의 일환으로 이 작업을 자동으로 처리합니다.

기계 학습 제품

AWS Marketplace에는 AWS Marketplace를 통해 구독할 수 있는 기계 학습 제품 카테고리가 있습니다. 이 제품 카테고리는 기계 학습입니다. 이 카테고리에 속하는 제품으로는 기계 학습(ML) 모델 패키지와 알고리즘이 있습니다.

수백 가지에 이르는 ML 모델 패키지와 알고리즘은 컴퓨터 비전, 자연어 처리, 음성 인식, 텍스트/데이터/음성/이미지/영상 분석, 사기 탐지, 예측 분석 등 광범위한 하위 범주에서 찾아 검색할 수 있습니다.

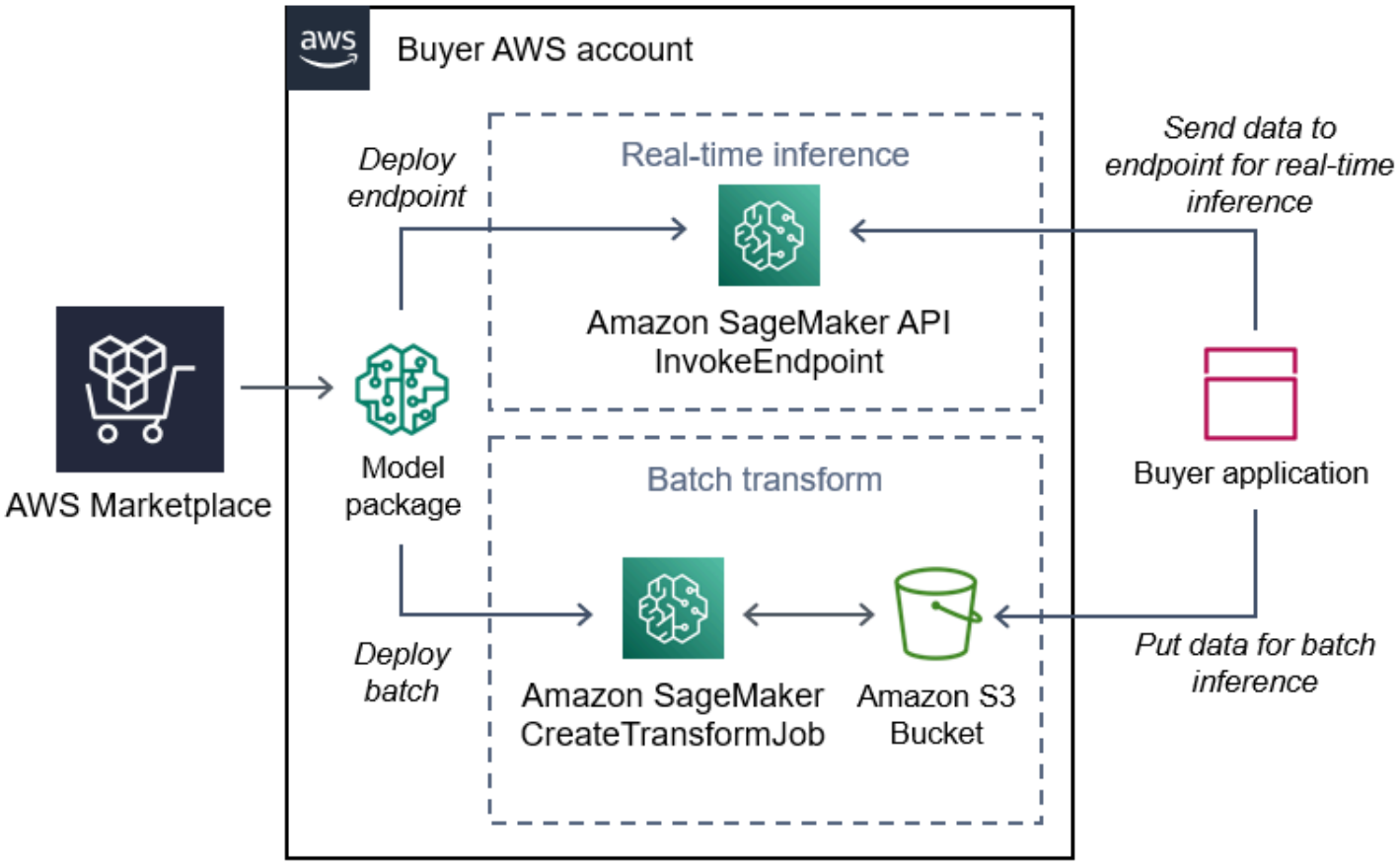
모델 품질 및 적합성을 평가하려면 제품 설명, 사용 지침, 고객 리뷰, Jupyter 노트북 샘플, 요금, 지원 정보 등을 살펴보는 것이 좋습니다. 모델은 Amazon SageMaker 콘솔에서 직접 배포하거나 Jupyter Notebook을 통해, Amazon SageMaker SDK를 사용하여 또는 AWS Command Line Interface AWS CLI를 사용하여 배포합니다. Amazon SageMaker는 모든 마켓플레이스 제품에서 정적 스캔을 실행하여 훈련 및 추론 작업을 실행할 수 있는 안전한 환경을 제공합니다.

Amazon SageMaker 모델 패키지

Amazon SageMaker 모델 패키지는 사전 학습된 고유한 ML 모델로, Amazon SageMaker의 Amazon 리소스 이름(ARN)으로 식별됩니다. 고객은 Amazon SageMaker에서 모델 패키지를 사용하여 모델을 생성합니다. 그런 다음 이 모델은 실시간 추론을 실행하는 호스팅 서비스에 사용하거나 Amazon SageMaker에서 배치 추론을 실행하는 배치 변환에 사용할 수 있습니다.

다음 다이어그램은 모델 패키지 제품을 사용하는 워크플로를 보여줍니다.

1. AWS Marketplace에서 모델 패키지 제품을 찾아 구독합니다.
2. SageMaker에서 제품의 추론 구성 요소를 배포하여 실시간으로 또는 일괄적으로 추론(또는 예측)을 수행합니다.

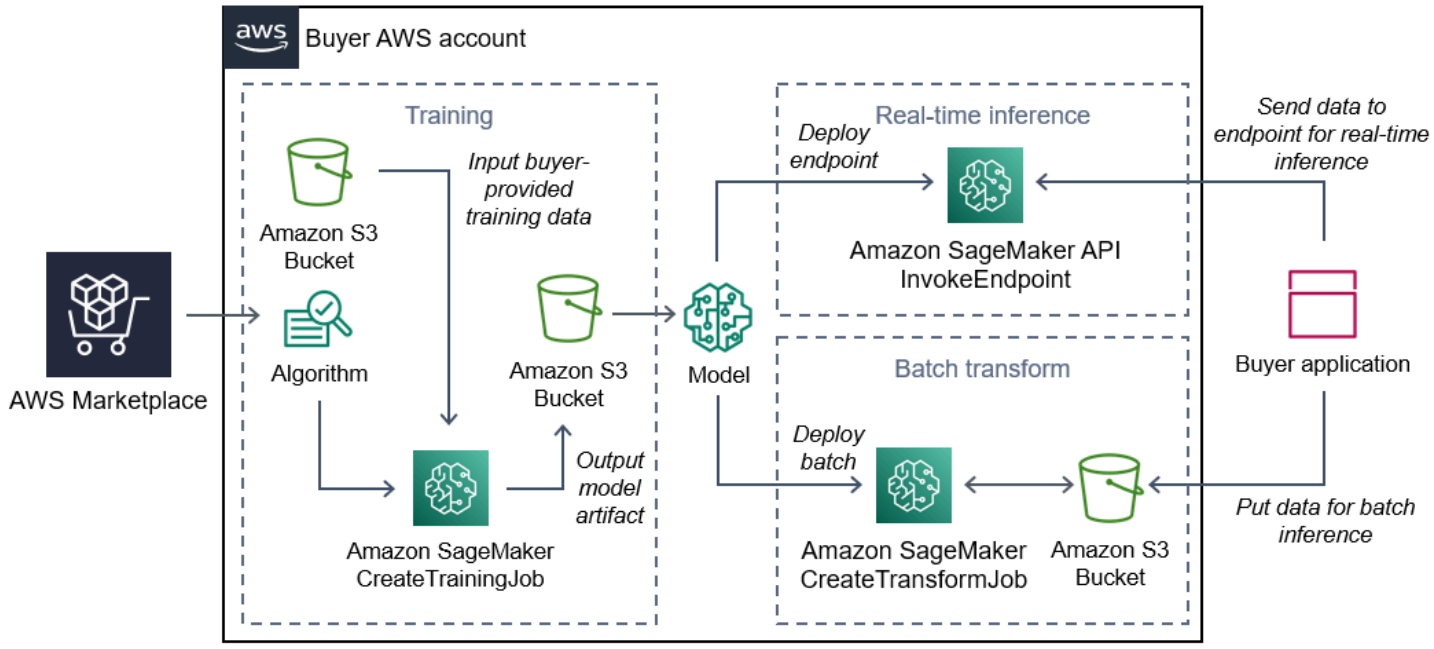


Amazon SageMaker 알고리즘

Amazon SageMaker 알고리즘은 ARN으로 식별되는 고유의 Amazon SageMaker 엔터티입니다. 여기에는 훈련과 추론, 두 가지의 논리 구성 요소가 있습니다.

다음 다이어그램은 알고리즘 제품을 사용하는 워크플로를 보여줍니다.

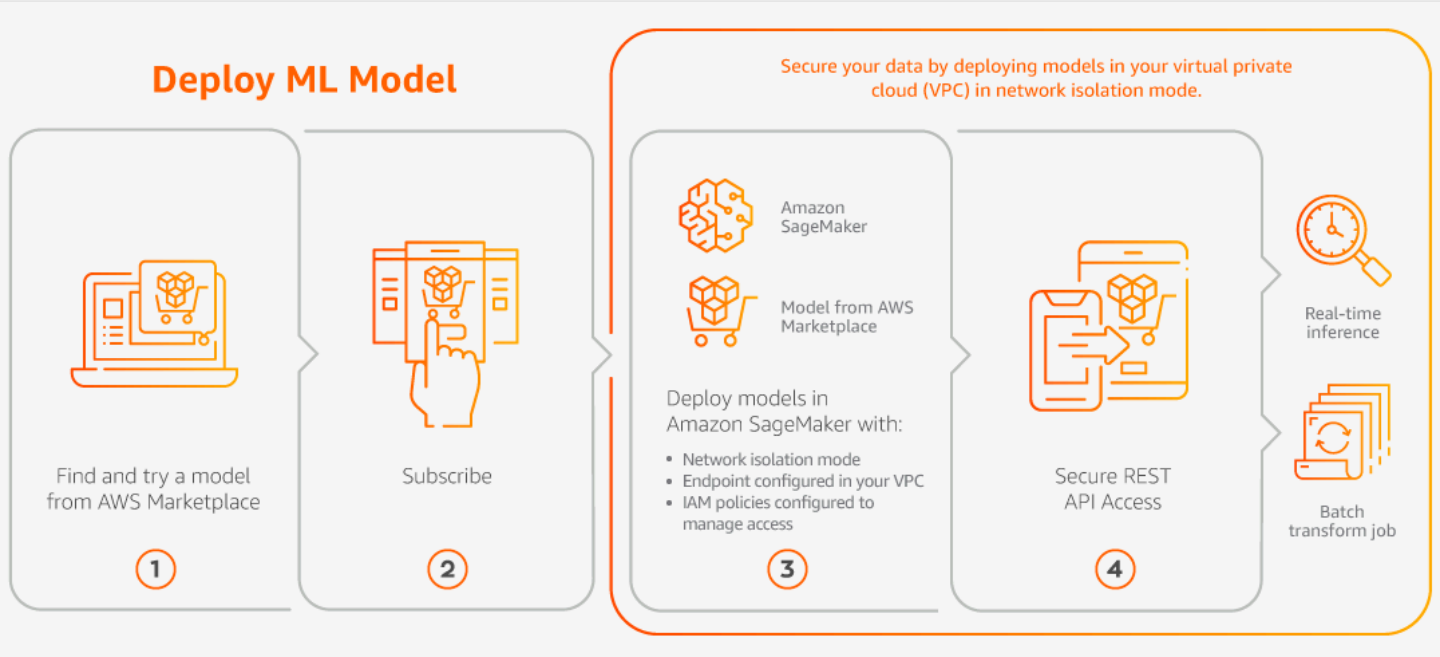
1. AWS Marketplace에서 알고리즘 제품을 찾아 구독합니다.
2. 제품의 훈련 구성 요소를 사용하여 Amazon SageMaker의 입력 데이터 세트를 사용하여 기계 학습 모델을 구축하는 훈련 작업 또는 튜닝 작업을 생성합니다.
3. 제품의 훈련 구성 요소가 완성되면 해당 구성 요소는 기계 학습 모델의 모델 아티팩트를 생성합니다.
4. SageMaker는 Amazon Simple Storage Service(S3) 버킷에 모델 아티팩트를 저장합니다.
5. 그 후 SageMaker에서 생성된 모델 아티팩트를 통해 제품의 추론 구성 요소를 배포하여 실시간으로 또는 일괄적으로 추론(또는 예측)을 수행합니다.



찾아서 구독한 후 배포하기

다음 다이어그램은 Amazon SageMaker에서 기계 학습 제품을 찾고, 구독하고, 배포하는 프로세스를 간략하게 보여줍니다.

1. AWS Marketplace에서 모델을 찾아 사용해보기
2. ML 제품 구독
3. Amazon SageMaker에서 모델 배포
4. 안전한 REST API 사용
5. 수행
   - 실시간 추론
   - 배치 변환 작업



요금은 사용량에 대해서만 지불하며, 최소 수수료 또는 선수금은 없습니다. AWS Marketplace에서는 알고리즘 및 모델 패키지와 AWS 인프라 사용 요금에 대한 통합 청구서를 제공합니다.

다음 섹션에서는 ML 제품을 찾고, 구독하고, 배포하는 방법을 설명합니다.

주제

- 기계 학습 제품 찾기
- 기계 학습 제품 구독
- 기계 학습 제품 배포

기계 학습 제품 찾기

Amazon SageMaker 모델 패키지 및 알고리즘을 찾는 방법

1. AWS Marketplace 웹 사이트에 로그인합니다.
2. 요건에 적합한 AWS Marketplace 제품 찾기에서 범주 드롭다운 메뉴를 사용하여 기계 학습 아래에서 원하는 하위 범주를 찾습니다.
3. 검색 결과는 리소스 유형, 카테고리, 요금 필터 등을 적용하여 새롭게 바꿀 수 있습니다.
4. 검색 결과에서 제품 세부 정보 페이지에 액세스합니다.
5. 제품 설명, 사용 지침, 고객 리뷰, 데이터 요구 사항, Jupyter Notebook 샘플, 요금 및 지원 정보를 검토합니다.

기계 학습 제품 구독

Amazon SageMaker 모델 패키지 및 알고리즘을 구독하는 방법

1. 제품 세부 정보 페이지에서 계속 구독하기를 선택합니다.
2. 조달 페이지에서 제품 요금 정보와 최종 사용자 라이선스 계약(EULA) 을 검토합니다.
3. 계속 구독하기를 선택합니다.

기계 학습 제품 배포

Amazon SageMaker 모델 패키지 및 알고리즘을 배포하는 방법

1. 내 Marketplace 소프트웨어로 이동하여 알고리즘 또는 모델 패키지에 대한 구독이 유효한지 확인합니다.
2. AWS Marketplace 웹 사이트에서 제품을 구성합니다(예: 특정 버전 또는 배포 리전을 선택하여).

   구매자가 모델 패키지 제품 또는 알고리즘 제품을 구독하면 해당 제품이 SageMaker 콘솔의 구매자 제품 목록에 추가됩니다. 구매자는 AWS SDK, AWS Command Line Interface(AWS CLI) 또는 SageMaker 콘솔을 사용하여 완전 관리형 REST 추론 엔드포인트를 생성하거나 데이터 배치에 대한 추론을 수행할 수도 있습니다.
3. Amazon SageMaker에서 보기를 선택하여 Amazon SageMaker 제품 세부 정보 페이지를 봅니다.
4. Amazon SageMaker 콘솔에서 Amazon SageMaker 콘솔, Jupyter Notebook, Amazon SageMaker CLI 명령 또는 API 작업을 사용하여 모델 패키지 및 알고리즘을 배포할 수 있습니다.

Amazon SageMaker에 배포하는 방법에 대한 자세한 내용은 시작하기를 참조하세요.

전문 서비스 제품

AWS Marketplace에는 AWS Marketplace 판매자가 제공하는 전문 서비스 제품이 있습니다. AWS Marketplace에서 검색할 때 전문 서비스 범주에서 이러한 제품을 찾을 수 있습니다. AWS Marketplace를 통해 이러한 제품을 구독하고 구매하지만, 판매자와 협의하여 요구 사항에 맞는 전문 서비스를 설정해야 합니다.

전문 서비스 구매

AWS Marketplace에서 전문 서비스 범주를 사용하여 전문 서비스를 검색할 수 있습니다. 원하는 제품을 찾았으면 판매자에게 제안을 요청하세요. 전문 서비스는 일반적으로 판매자와 협의가 필요하므로,

구매를 완료하려면 판매자에게 몇 가지 추가 정보를 제공해야 합니다. 이 기회를 잘 활용하여 요금 및 해결해야 할 기타 서비스 세부 사항을 협상할 수도 있습니다. 제품에 대한 비공개 제안을 받게 됩니다. 비공개 제안에 대한 자세한 내용은 비공개 제안 섹션을 참조하세요.

전문 서비스 제품을 구매하는 방법

1. AWS Marketplace로 이동하여 AWS 계정으로 로그인한 다음, 구매하려는 전문 서비스 제품을 검색하여 찾습니다.
2. 제품 세부 정보 페이지에서 계속을 선택합니다.
3. 서비스 요청 페이지에서 구매자의 이름, 이메일 주소, 회사 이름, 판매자에게 도움이 되는 추가 정보(비즈니스 요구 사항, 일정, 계약 요구 사항 등)를 포함하여 판매자가 제안을 생성하는 데 필요한 추가 정보를 입력합니다.
4. 판매자는 구매자가 입력한 이메일 주소를 통해 구매자에게 연락하여 제안의 세부 사항을 협의합니다. 구매자가 동의하면 판매자는 AWS Marketplace의 제안으로 연결되는 링크를 구매자에게 보냅니다. 브라우저에서 링크를 열고 AWS 계정에 로그인합니다.
5. 조달 페이지를 열고 판매자의 제안 세부 사항을 검토합니다. 해당 제안이 기대하는 서비스에 부합하고 요금이 적절한 수준인지 확인합니다. 조건(예: 일시불 결제인지 아니면 일련의 요금을 지불하는 방식인지)도 확인합니다. 제안이 마음에 들면 계속 진행합니다. 그렇지 않으면 판매자에게 연락하여 변경합니다.
6. 계약 구성에서 계약에 사용하려는 구성을 선택합니다. 예를 들어 지원 계약을 구매하는 경우 각각 가격이 다른 Silver, Gold 또는 Platinum 계약 옵션이 있을 수 있습니다.
7. 서비스를 구매하려면 계약 생성을 선택합니다. 그러면 판매자가 2영업일 이내에 연락하여 서비스 사용 지침을 제공합니다.

SaaS 제품

서비스형 소프트웨어(SaaS) 제품의 경우 AWS Marketplace를 통해 제품을 구독하지만 소프트웨어 판매자의 환경에서 제품에 액세스합니다.

주제

- 요금 모델
- 빠른 시작

요금 모델

AWS Marketplace에서는 다음과 같은 가격 책정 모델을 제공합니다.

SaaS 사용량 기반 구독

SaaS 사용량 기반 구독에서는 소프트웨어 판매자가 사용량을 추적하고, 고객은 사용한 만큼 요금을 지불합니다. 이 사용량에 따른 요금 모델은 여러 AWS 서비스 서비스의 요금 모델과 비슷합니다. SaaS 제품 사용량에 대한 청구는 AWS 청구서를 통해 관리합니다.

SaaS 사용량 기반 구독을 사용하여 구독하려면

1. 제품 세부 정보 페이지에서 구매 옵션 보기를 선택하여 구독 프로세스를 시작합니다.
2. 구독을 검토하고 구독 페이지에서 구독을 선택합니다.

> **Note**
>
> 일부 제품은 소프트웨어를 구성, 배포 및 시작하는 데 필요한 시간과 리소스를 줄이는 빠른 시작 배포 옵션을 제공합니다. 이러한 제품은 빠른 시작 배지를 사용하여 식별됩니다. 자세한 내용은 the section called “빠른 시작” 섹션을 참조하세요.

SaaS 선결제 약정

일부 회사는 AWS Marketplace에서 구매하는 제품에 SaaS 선결제 계약을 제공합니다. 이 옵션을 선택하면 개별 수량의 라이선스를 구매하거나 해당 제품에 대한 데이터를 수집할 수 있습니다. 그러면 AWS 계정을 통해 해당 제품의 요금을 미리 청구할 수 있습니다. 예를 들어 연간 사용자 액세스 라이선스를 10개 구매하거나, 혹은 연간 1일 데이터 수집 크기를 10GB 구매할 수 있습니다.

제품을 구매하면 빠른 시작이 활성화되어 있지 않은 경우 계정 설정 및 구성을 위해 해당 제품의 웹 사이트로 이동됩니다. 이후부터는 정기 AWS 계정 청구서에 사용 요금이 표시됩니다.

> **Note**
>
> 빠른 시작 환경에 대한 자세한 내용은 the section called “빠른 시작” 섹션을 참조하십시오.

SaaS 계약으로 구독하는 방법

1. 제품 세부 정보 페이지에서 구매 옵션 보기를 선택하여 구독 프로세스를 시작합니다. 원하는 수량 또는 단위, 구독 기간(여러 옵션이 제공되는 경우), 자동 갱신을 선택할 수 있습니다.
2. 선택을 마치면 Create Contract(계약 생성)를 선택합니다.
3. Set Up Your Account(계정 설정)을 선택하고 해당 회사의 웹사이트로 이동합니다. 계정을 구성하고 결제를 확인하는 동안 제품에 대한 AWS Marketplace 세부 정보 페이지에서 계약이 보류 중임을 확인할 수 있습니다.

> **Note**
>
> 일부 제품은 소프트웨어를 구성, 배포 및 시작하는 데 필요한 시간과 리소스를 줄이는 빠른 시작 배포 옵션을 제공합니다. 이러한 제품은 빠른 시작 배지를 사용하여 식별됩니다. 자세한 내용은 the section called “빠른 시작” 섹션을 참조하세요.

구성이 완료되면 제품 페이지에서 계정을 설정하는 링크를 사용할 수 있게 됩니다. AWS Marketplace 계정에 로그인하면 내 Marketplace 소프트웨어 아래에 소프트웨어가 표시됩니다. 이제 소프트웨어를 사용할 수 있습니다. 계정에 대한 설정 프로세스를 완료하지 않으면 AWS Marketplace에서 해당 제품을 다시 방문할 때 완료하라는 메시지가 표시됩니다.

소프트웨어 회사의 웹 사이트에서 만든 계정을 사용해 소프트웨어 구독에 액세스합니다. 또한 AWS Marketplace 계정에 로그인하면 AWS Marketplace를 통해 구매한 소프트웨어 구독의 웹 사이트 링크를 Marketplace 소프트웨어 아래에서 찾을 수 있습니다.

SaaS 무료 평가판

일부 공급업체는 평가 목적으로 AWS Marketplace를 통해 SaaS 제품의 무료 평가판을 제공합니다. AWS Marketplace에서 SaaS 제품을 검색하고 결과를 필터링하여 무료 평가판이 제공되는 제품만 표시할 수 있습니다. 검색 결과에는 어떤 제품이 무료 평가판을 제공하는지 표시됩니다. 모든 무료 평가판 제품은 제품 로고 옆에 무료 평가판 배지가 표시됩니다. 제품 조달 페이지에서 무료 평가판 기간 및 평가판에 포함된 무료 소프트웨어 사용량을 확인할 수 있습니다.

무료 평가판 기간 중 또는 무료 평가판이 만료된 후에는 비공개 제안을 협상하거나 공개 제안을 구독하여 구매 결정을 내릴 수 있습니다. SaaS 무료 평가판은 자동으로 유료 계약으로 전환되지 않습니다. 무료 평가판이 더 이상 필요 없으면 무료 평가판이 만료되도록 두면 됩니다.

AWS Marketplace 콘솔에서 구독 관리를 선택하여 구독을 확인할 수 있습니다.

> **Note**
>
> 각 AWS 계정은 제품당 1개의 무료 평가판만 이용할 수 있습니다.

SaaS 계약 무료 평가판 제안 구독

SaaS 계약 무료 평가판 제안을 구독하는 방법

1. AWS Marketplace 콘솔에 로그인하고 AWS Marketplace 메뉴에서 제품 검색을 선택합니다.
2. 결과 구체화 패널에서 무료 평가판으로 이동하여 무료 평가판을 선택합니다.
3. 제공 방법으로 SaaS를 선택합니다.
4. 요금 모델에서 선불 약정을 선택하여 무료 평가판을 제공하는 모든 제품을 확인합니다. 모든 적격 제품에는 무료 평가판 배지가 표시됩니다.
5. 원하는 SaaS 제품을 선택합니다.
6. 제품 세부 정보 페이지에서 무료 시험 사용을 선택합니다.
7. 제안 유형에서 무료 평가판 옵션을 선택합니다.
8. 구매에서 계약 생성을 선택하고 계약 수락을 선택합니다.
9. 계정 설정을 선택하여 등록을 완료하고 소프트웨어 사용을 시작합니다.

SaaS 구독 무료 평가판 제안 구독

SaaS 구독 무료 평가판 제안을 구독하는 방법

1. AWS Marketplace 콘솔에 로그인하고 AWS Marketplace 메뉴에서 제품 검색을 선택합니다.
2. 결과 구체화 패널에서 무료 평가판으로 이동하여 무료 평가판을 선택합니다.
3. 제공 방법으로 SaaS를 선택합니다.
4. 요금 모델에서 사용량 기반을 선택하여 무료 평가판을 제공하는 모든 제품을 확인합니다. 모든 적격 제품에는 무료 평가판 배지가 표시됩니다.
5. 원하는 SaaS 제품을 선택합니다.
6. 제품 세부 정보 페이지에서 무료 시험 사용을 선택합니다.
7. 제안 유형에서 무료 평가판 옵션을 선택합니다.
8. 구매에서 구독을 선택합니다.

빠른 시작

빠른 시작은 빠른 시작이 활성화된 SaaS 제품에 사용할 수 있는 AWS Marketplace 배포 옵션입니다. 소프트웨어를 구성, 배포 및 시작하는 데 필요한 시간, 리소스 및 단계를 줄여줍니다. 이 기능을 제공하는 제품의 경우 빠른 시작을 사용하거나 리소스를 수동으로 구성할 수 있습니다.

빠른 시작 환경을 사용하여 SaaS 제품을 찾고, 구독하고, 출시하려면

1. AWS Marketplace 검색 페이지로 이동합니다.
2. AWS Marketplace를 찾은 다음, 시작하려는 소프트웨어가 포함된 제품을 찾습니다. 빠른 시작 환경을 제공하는 제품의 제품 설명에는 빠른 시작 배지가 있습니다.

   > **Tip**
   >
   > 빠른 시작 환경이 활성화된 제품을 찾으려면 결과 세분화 창에서 SaaS 및 CloudFormation 템플릿 필터를 사용하십시오.

3. 제품을 구독한 후 계정 설정 버튼을 선택하여 구성 및 시작 페이지로 이동합니다.
4. 구성 및 시작 페이지의 1단계: 필요한 AWS 권한이 있는지 확인에서 빠른 시작 환경을 사용하는 데 필요한 권한이 있는지 확인하십시오. AWS 관리자에게 문의하여 권한을 요청하십시오.

   전체 빠른 시작 환경을 사용하려면 다음 권한이 있어야 합니다.

   - `CreateServiceLinkedRole` - AWS Marketplace에게 `AWSServiceRoleForMarketplaceDeployment` 서비스 연결 역할 생성을 허용합니다. 이 서비스 연결 역할을 통해 AWS Marketplace에서 AWS Secrets Manager에 보안 정보로 저장되는 배포 관련 파라미터를 사용자 대신 관리할 수 있습니다.
   - `DescribeSecrets` - AWS Marketplace에서 판매자가 전달한 배포 파라미터에 대한 정보를 얻을 수 있습니다.
   - `GetRole` - AWS Marketplace에서 계정에 서비스 연결 역할이 생성되었는지 확인할 수 있습니다.
   - `ListSecrets` - AWS Marketplace에서 배포 파라미터의 상태를 확인할 수 있습니다.
   - `ListRegions` - AWS Marketplace에서 현재 계정에 옵트인된 AWS 리전을 가져올 수 있습니다.
   - `ReplicateSecrets` - AWS Marketplace에서 소프트웨어를 배포할 선택 지역으로 암호 복제를 시작할 수 있습니다.

5. 2단계: 기존 또는 새 공급업체 계정에 로그인에서 로그인 또는 계정 만들기 버튼을 선택합니다. 판매자의 사이트가 새 탭에서 열리며, 여기서 로그인하거나 새 계정을 만들 수 있습니다. 작업을 마치면 구성 및 시작 페이지로 돌아갑니다.
6. 3단계: 소프트웨어 및 AWS 통합 구성에서 원하는 제품 구성 방법을 선택합니다.
   - AWS CloudFormation - 템플릿 실행 버튼을 선택하여 사전 정의된 CloudFormation 템플릿을 배포하여 제품을 구성합니다. CloudFormation을 사용하여 템플릿 파라미터를 검토하고 추가 필수 필드를 모두 작성합니다. 작업을 마치면 구성 및 시작 페이지로 돌아가 소프트웨어를 시작합니다.
   - 수동 - 판매자가 제공한 지침을 사용하여 소프트웨어를 구성합니다.
7. 4단계: 소프트웨어 시작에서 소프트웨어 시작 버튼을 선택하여 소프트웨어를 시작합니다.

데이터 제품

AWS Marketplace를 사용하여 AWS Data Exchange를 통해 사용 가능한 데이터 제품을 찾고 구독할 수 있습니다. 자세한 내용은 AWS Data Exchange 사용 설명서의 AWS Data Exchange에서 데이터 제품 구독을 참조하세요.

제품 요금 납부

월초에 Amazon Web Services(AWS)로부터 AWS Marketplace 요금 청구서를 받게 됩니다. 소프트웨어 제품의 경우, 이 소프트웨어에 설치된 Amazon Machine Image(AMI) 인스턴스가 실행된 시간에 소프트웨어의 시간당 요금을 곱한 금액이 청구서에 포함됩니다. Amazon Elastic Compute Cloud(Amazon EC2), Amazon Simple Storage Service(S3), Amazon Elastic Block Store(Amazon EBS) 등의 AWS 인프라 서비스 및 대역폭 사용 요금 청구서도 받게 됩니다.

AWS 계정 위치가 터키와 남아프리카 공화국을 제외한 유럽, 중동 및 아프리카(EMEA)이고 EMEA 적격 판매자로부터 제품을 구매한 경우 Amazon Web Services EMEA SARL(AWS Europe)로부터 청구서를 받게 됩니다. 그렇지 않으면 AWS Inc.로부터 청구서를 받게 됩니다.

> **Note**
>
> 계약 구매의 경우 통합 월별 청구서가 아닌 구독 시점에 구독 요금이 청구됩니다. 유연한 계약 결제는 예정된 결제 시점에 청구됩니다. 사용량 구성 요소가 있는 계약(예: 사용한 만큼만 지불 모델)의 경우 사용량이 통합 월별 청구서에 표시됩니다.

복잡한 토폴로지를 사용하는 AWS Marketplace 제품은 제공된 AWS CloudFormation 템플릿이 시작한 AMI 클러스터 및 기타 AWS 인프라 서비스 요금이 부과될 수 있습니다.

예를 들어 EC2 스몰 인스턴스 유형에서 소프트웨어를 720시간 실행한다고 가정하겠습니다. 판매자의 소프트웨어 사용 요금은 시간당 0.12 USD이고 EC2 요금은 시간당 0.085 USD입니다. 매달 말에 147.60 USD가 청구됩니다.

데이터 제품 구독에 대한 자세한 내용은 AWS Data Exchange 사용 설명서의 AWS Data Exchange에서 데이터 제품 구독을 참조하세요.

AWS 청구서 요금 납부에 대한 자세한 내용은 AWS Billing 사용 설명서를 참조하세요.

Amazon Web Services EMEA SARL(AWS Europe)에서 결제 관리에 대한 자세한 내용은 AWS Billing 사용 설명서의 AWS Europe에서 결제 관리를 참조하세요.

주제

- 제품 구독 취소
- 결제 방법
- 지원되는 통화
- 기본 통화 변경
- 송금 지침 업데이트

구매 주문

AWS Marketplace 및 AWS Billing 콘솔에서 구매 주문을 사용하면 고객이 정의한 구매 주문 번호가 포함된 인보이스를 AWS로부터 받게 됩니다. 이 접근 방식은 결제 처리 및 비용 할당이 간단합니다. AWS Marketplace에서 비정기 인보이스에는 즉시 요금이 청구되는 구매 또는 비공개 제안에 정의된 결제 일정에 따라 요금이 청구되는 구매가 포함됩니다. 일반적으로 사용한 만큼만 지불 요금이 통합 AWS Marketplace 월별 사용 인보이스에 표시됩니다.

AWS Marketplace 거래에 구매 주문 사용

거래 시 구매 주문을 추가할 수 있으며, 이는 해당 거래와 관련된 모든 후속 비정기 인보이스에 적용됩니다.

구매 주문을 지원하는 제품은 다음과 같습니다.

- 서비스형 소프트웨어(SaaS) 계약
- 전문 서비스 제품
- 서버 제품(연간 또는 계약 요금 모델이 적용되는 AMI 인스턴스, 컨테이너, AWS CloudFormation 템플릿 및 차트 Helm 포함)

> **Note**
>
> 연간 요금 모델에 대한 구매 주문 지원은 유연한 결제 일정이 적용되는 비공개 제안에만 제공됩니다.

연간 요금 모델에 대한 구매 주문 지원은 유연한 결제 일정이 적용되는 비공개 제안에만 제공됩니다. 구매자가 지정하는 구매 주문은 사용한 만큼만 지불 요금의 통합 AWS Marketplace 월별 인보이스에 적용되지 않습니다.

> **Note**
>
> AWS Marketplace에서 구매 주문을 사용하려면 AWS 조직의 관리 계정에서 AWS Billing 통합을 활성화해야 합니다. 이 일회성 설정 작업을 통해 서비스 연결 역할이 생성되며, 그러면 구독 권한이 있는 조직 내 계정에서 구매 주문을 사용할 수 있습니다. 통합을 활성화하지 않으면 조직 내 계정에서 조달 중에 구매 주문을 추가할 수 없습니다. 통합에 대한 자세한 내용은 AWS Marketplace에 대한 서비스 연결 역할 생성을 참조하세요.

AWS Marketplace에서 구매 주문을 지정하는 방법

1. AWS Marketplace에서 지원되는 제품을 찾아 구매할 준비를 합니다.
2. 구매 프로세스 중에 소프트웨어 구독 구성 페이지(SaaS의 경우)의 구매 주문에서 구매 주문 번호 추가를 선택합니다.
3. 구매 주문 번호 필드에 구매 주문 번호를 입력합니다.

   구매 주문 번호는 시스템에서 구매 주문을 추적하는 데 사용되는 번호 또는 텍스트입니다. 일반적으로 내부 시스템 또는 프로세스에서 발행합니다. 최대 길이는 200자입니다.

AWS Marketplace 거래 중에 제공된 구매 주문을 포함하여 구매 주문에 대한 자세한 내용을 보려면 AWS Billing 콘솔의 구매 주문 대시보드를 사용하세요.

일괄 사용량 구매 주문 사용

AWS Marketplace 요금을 다른 구매 주문과 분리하려면 AWS Billing 콘솔에서 AWS Marketplace 일괄 사용량 품목이 포함된 구매 주문을 생성하면 됩니다. AWS Marketplace 인보이스 거래에는 특정 조건과 파라미터가 일치하는 경우(예: 청구 주체) 구매자가 지정하는 일괄 사용량 구매 주문이 포함됩니다. 단, AWS Marketplace 거래 구매 주문이 지정된 비정기 청구서는 예외입니다. 자세한 내용은 AWS 과금 정보 및 비용 관리 사용 설명서의 구매 주문 관리를 참조하세요.

구매 주문 문제 해결

다음 표의 정보는 구매 주문과 관련된 문제를 해결하거나 다른 시나리오에서 발생하는 상황을 이해하는 데 도움이 될 수 있습니다.

시나리오	세부 정보
권한 부족	구독할 수 있는 `aws-marketplace:Subscribe` 권한이 없는 경우 구매 주문 입력 필드 근처에 메모가 표시됩니다. 또한 관리 계정에서 AWS Billing 통합을 활성화해야 합니다. 통합 활성화에 대한 자세한 내용은 AWS Marketplace에 대한 서비스 연결 역할 생성을 참조하세요.
구매 주문이 없음	AWS Marketplace가 자동으로 새 구매 주문을 생성합니다. 새 구매 주문에는 기본 정보만 있고 연락처 정보가 없습니다.
구매 주문 알림 누락	연락처 정보가 없는 구매 주문(AWS Marketplace가 생성한 구매 주문 포함)은 이메일 알림을 받을 수 없습니다. 과금 정보 및 비용 관리 콘솔의 구매 주문 대시보드에서 구매 주문에 연락처 정보를 추가할 수 있습니다.
잘못된 구매 주문 번호를 추가함	잘못된 구매 주문 번호를 입력하여 업데이트가 필요한 경우 AWS Support에 문의하여 구매 주문 번호를 업데이트합니다.
구독 계정이 다른 조직으로 이전됨	새 조직에서 구매 주문이 작동하려면 새 조직에서 통합을 완료해야 합니다. 통합이 완료되고 새 조직에서 구매 주문 지원이 작동하면 구독하는 계정이 조직 간에 이전될 때 새 인보이스에 새 조직의 구매 주문 번호가 표시됩니다(그리고 필요한 경우 새 구매 주문이 생성됨).
체크아웃할 때 구매 주문 옵션을 사용할 수 없음	AWS Billing 통합은 SaaS 계약, 전문 서비스 제품, 계약 가격이 적용되는 서버 제품, 유연한 결제 일정이 적용되는 비공개 제안의 연간 요금이 적용되는 서버 제품에만 사용할 수 있습니다.
사용한 만큼만 지불 계약	계약 인보이스에는 구매 주문 번호가 표시되지만 소비 인보이스(사용한 만큼만 지불)에는 구매 주문 번호가 표시되지 않습니다. 사용한 만큼만

시나리오	세부 정보
	지불 모델은 구매 주문 번호를 추가할 수 없습니다. AWS Billing 콘솔에서 AWS Marketplace 일괄 사용량 품목이 포함된 구매 주문을 추가하는 것을 고려해 보세요.
구매 주문이 일시 중단됨	구매 주문 번호를 입력한 후 과금 정보 및 비용 관리 콘솔의 구매 주문 대시보드에서 구매 주문이 일시 중단된 것으로 표시되면 새 품목이 구매 주문에 추가되었지만 인보이스에는 구매 주문이 없는 것입니다. AWS 계정의 청구 관리자는 구매 주문을 활성화하고 AWS Support에 문의하여 활성 구매 주문으로 인보이스를 다시 생성해야 합니다.
구매 주문이 만료됨	구매 주문 번호를 입력한 후 구매 주문이 만료되면 새 품목이 생성되고 구매 주문이 활성 상태로 표시됩니다. 품목의 종료 날짜가 새 구매 주문 만료 날짜로 사용됩니다.
잔액 추적	AWS Marketplace 품목에는 잔액 추적이 활성화되지 않습니다.
조달 시스템 통합	통합 조달 시스템에서 제공하는 구매 주문은 인보이스에 표시됩니다.
유연한 결제 일정 - 최초 구매	인보이스 발행 날짜가 지정된 계약(유연한 결제 일정)은 구매 주문에 0 USD의 최초 품목을 생성합니다. 각 인보이스에는 해당 요금이 적용된 추가 품목이 생성됩니다.
유연한 결제 일정 - 여러 구매 주문	유연한 결제 일정의 개별 결제를 여러 구매 주문과 함께 표시하려면 AWS Support에 문의하여 향후 인보이스의 구매 주문 번호를 변경합니다.

환급에 관한 정보

고객은 AWS Marketplace 제품과 관련하여 다양한 종류의 환불을 요청할 수 있습니다. AWS에서 판매한 AWS Marketplace 제품의 경우 환불 정책 페이지를 살펴본 후 AWS Support Center Console을 사용하여 지원 문의 양식을 제출하세요. 제품을 타사에서 판매한 경우 해당 제품 세부 정보 페이지의 환불 정책을 검토하세요. AWS Marketplace 구독의 소프트웨어 요금은 제품 판매자에게 지급되며, 환불은 판매자에게 직접 요청해야 합니다. 각 AWS Marketplace 판매자는 AWS Marketplace 페이지에 환불 정책을 포함해야 합니다.

AWS Marketplace 구매와 관련된 환불에 대한 자세한 내용은 AWS Marketplace 판매자 설명서의 다음 주제를 참조하세요.

- 환불
- 제품 요금

> **Note**
>
> 비공개 제안과 관련된 모든 환급은 판매자에게 문의하십시오.

제품 구독 취소

AWS Marketplace에서 제품 구독을 취소하거나 자동 갱신할 수 있습니다. 다음 단계에서는 AWS Marketplace의 서비스형 소프트웨어(SaaS), 기계 학습(ML) 및 Amazon Machine Image(AMI) 제품에 대한 지침을 제공합니다.

주제

- SaaS 구독 취소
- 기계 학습 구독 취소
- AMI 구독 취소
- SaaS 계약 구독의 자동 갱신 취소

SaaS 구독 취소

1. AWS Management Console에 로그인하고 AWS Marketplace 콘솔을 엽니다.

2. 구독 관리 페이지로 이동합니다.
3. 제공 방법 드롭다운 목록에서 SaaS를 선택합니다.
4. 취소할 제품의 구독을 선택합니다.
5. 구독 취소를 선택합니다.

기계 학습 구독 취소

기계 학습 구독을 취소하기 전에, 다음 조치를 수행합니다.

- ML 알고리즘인 경우 AWS Management Console에 로그인하고 Amazon SageMaker 콘솔을 엽니다. 알고리즘에 대해 실행 중인 학습 작업을 종료합니다. 알고리즘에서 모델 패키지를 생성한 경우 기계 학습 구독을 취소한 후에는 실시간 엔드포인트를 시작하거나 배치 추론 작업을 생성할 수 없습니다.
- 알고리즘에서 생성한 ML 모델 패키지 또는 모델인 경우 AWS Management Console에 로그인하고 Amazon SageMaker 콘솔을 엽니다. 모델에 대해 실행 중인 실시간 엔드포인트를 종료하거나 실행 중인 배치 추론 작업을 종료합니다.

> **Note**
>
> 종료되지 않은 기존 작업과 엔드포인트는 계속 실행되며 종료될 때까지 요금이 청구됩니다.

기계 학습 구독을 취소하는 방법

1. AWS Management Console에 로그인한 다음 AWS Marketplace 콘솔을 엽니다.
2. 내 구독 페이지로 이동합니다.
3. 취소할 제품의 구독을 선택합니다.
4. 구독 취소를 선택합니다. 구독을 취소한 후에는 알고리즘 또는 모델을 시작할 수 없습니다.

AMI 구독 취소

1. AWS Management Console에 로그인한 다음 AWS Marketplace 콘솔을 엽니다.
2. 구독 관리 페이지로 이동합니다.
3. 제공 방법 드롭다운 목록에서 Amazon Machine Image를 선택합니다.
4. 취소할 제품의 구독을 선택합니다.
5. 작업 드롭다운 목록에서 구독 취소를 선택합니다.

6. 제공되는 정보를 읽고 실행 중인 인스턴스 요금이 계정에 청구됨을 확인하고 확인란을 선택합니다. 예, 구독 취소를 선택합니다.
7. AWS 콘솔에서 관리를 새 탭에서 엽니다.
8. Amazon EC2 콘솔에서 실행 중인 인스턴스를 종료합니다. 실행 중인 인스턴스가 여러 개 있는 경우 모두 종료해야 합니다. 또한 해당하는 경우 AWS CloudFormation 스택을 삭제해야 합니다.
9. 구독 관리 탭으로 돌아가서 예, 구독 취소를 선택합니다. 구독을 취소하면 소프트웨어에 액세스할 수 없게 되며 더 이상 소프트웨어 요금이 청구되지 않습니다.

SaaS 계약 구독의 자동 갱신 취소

1. AWS Management Console에 로그인한 다음 AWS Marketplace 콘솔을 엽니다.
2. 제품 세부 정보 페이지로 이동합니다.
3. 계속을 선택하여 주문 페이지로 이동합니다.
4. 갱신 수정 탭을 선택하고 갱신 취소를 선택합니다.

결제 방법

AWS 계정을 처음 생성할 때 해당 계정의 결제 방법을 설정합니다. AWS 과금 정보 및 비용 관리 콘솔에서 결제 방법을 관리할 수 있습니다. 자세한 지침은 AWS Billing 사용 설명서의 결제 관리를 참조하세요.

결제 오류

지급인 계정을 통해 결제를 처리하는 동안 오류가 발생하면 결제 방법을 업데이트하고 다시 시도하세요. 다음과 같은 이유로 오류가 발생할 수 있습니다.

- 결제 방법이 없거나 유효하지 않거나 지원되지 않습니다.
- 결제가 거부되었습니다.
- Amazon Internet Services Private Limited(AISPL) 계정이 계약 요금 모델이 적용되는 신규 구매에 직불 카드 또는 신용 카드를 사용할 수 없도록 제한합니다. AISPL 계정이 있는 경우 AWS 고객 서비스에 문의하여 기본 결제 방법을 업데이트하세요. 자세한 내용은 AWS Marketplace 블로그 웹 사이트의 Restriction on credit and debit card purchases for AISPL customers using AWS Marketplace를 참조하세요.
- 비공개 제안에 결제 일정이 포함되어 있습니다. 하지만 기본 결제 방법이 인보이스 발행 조건으로 설정되지 않았습니다.

업데이트된 결제 방법을 신규 구매에 사용할 수 있게 될 때까지 최대 7일이 걸릴 수 있습니다. 문제 해결에 도움이 필요하면 AWS Support에 문의하세요.

지원되는 통화

다음 목록에는 AWS 및 Amazon Web Services EMEA SARL에 지원되는 기존 통화가 모두 포함되어 있습니다.

> **Note**
>
> Amazon Internet Services Private Limited(AISPL)는 현재 AWS Marketplace에서 지원되지 않으므로 인도 루피(INR)는 지원되지 않습니다. 자세한 내용은 AWS 계정과 AISPL 계정의 차이점은 무엇입니까?를 참조하세요.

Amazon Web Services에서 지원되는 통화는 다음과 같습니다.

- 호주 달러(AUD)
- 영국 파운드(GBP)
- 캐나다 달러(CAD)
- 덴마크 크로네(DKK)
- 유로(EUR)
- 홍콩 달러(HKD)
- 일본 엔(JPY)
- 뉴질랜드 달러(NZD)
- 노르웨이 크로네(NOK)
- 싱가포르 달러(SGD)
- 남아프리카 랜드(ZAR)
- 스웨덴 크로나(SEK)
- 스위스 프랑(CHF)
- 미국 달러(USD)

Amazon Web Services EMEA SARL에서 지원되는 통화는 다음과 같습니다.

- 영국 파운드(GBP)

- 덴마크 크로네(DKK)
- 유로(EUR)
- 노르웨이 크로네(NOK)
- 남아프리카 랜드(ZAR)
- 스웨덴 크로나(SEK)
- 스위스 프랑(CHF)
- 미국 달러(USD)

기본 통화 변경

AWS Marketplace 구매 금액은 구매자가 AWS 계정에 대해 지정한 통화로 표시됩니다. AWS Billing and Cost Management 콘솔에서 계정의 기본 통화를 변경할 수 있습니다. 자세한 지침은 AWS Billing 사용 설명서의 청구서 결제에 사용되는 통화 변경을 참조하세요.

> **Note**
>
> 기본 통화를 변경하면 송금 지침이 변경됩니다. 업데이트된 송금 지침을 보려면 AWS Marketplace 인보이스를 확인하거나 AWS Billing and Cost Management 콘솔의 계정 설정 페이지를 참조하세요.

송금 지침 업데이트

AWS 계정 위치가 터키와 남아프리카 공화국을 제외한 유럽, 중동 및 아프리카(EMEA)이고 EMEA 적격 판매자로부터 제품을 구매한 고객은 Amazon Web Services EMEA SARL로부터 청구서를 받게 됩니다. Amazon Web Services EMEA SARL(AWS Europe) 인보이스의 송금 지침은 AWS, Inc.의 송금 지침과 다릅니다. AWS Billing and Cost Management 콘솔에 로그인하면 청구서에서 송금 정보를 찾을 수 있습니다. 인보이스의 송금 정보 부분에 표시되는 은행 계좌는 Amazon Web Services EMEA SARL을 통해 이루어지는 AWS 클라우드 서비스 구매와 다릅니다. Amazon Web Services EMEA SARL은 룩셈부르크의 공인 전자 화폐 기관인 Amazon Payments Europe, S.C.A.를 AWS Marketplace 인보이스 결제 처리자로 사용합니다. 모든 인보이스는 전액 정산되어야 합니다. 결제 금액이 인보이스 금액에 미달하면 구매자의 은행 계좌로 환불됩니다.

다음 표에는 거래 유형, 거래 주체 및 해당 송금 지침(인보이스의 자동 이체 세부 정보에 계정 이름이 표시됨)이 간략하게 설명되어 있습니다.

거래 유형	거래 주체	송금 지침
AWS 클라우드 서비스 구매	Amazon Web Services EMEA SARL	Amazon Web Services EMEA SARL
적격 AWS Marketplace 판매자	Amazon Web Services EMEA SARL	Amazon Payments Europe, S.C.A.
부적격 AWS Marketplace 판매자	AWS Inc.	AWS

송금 지침에 대한 은행 서류를 요청하려면 결제 또는 계정 지원을 선택하고 AWS에 문의에서 계정 및 결제 지원 사례를 생성하거나 <awslux-receivables-support@email.amazon.com>으로 이메일 메시지를 보내세요.

기본 통화를 지원되는 통화로 변경하는 방법에 대한 자세한 내용은 AWS Billing 사용 설명서의 청구서 결제에 사용되는 통화 변경을 참조하세요.

Amazon Web Services EMEA SARL은 전자 자금 이체, MasterCard, VISA 및 American Express 신용카드 결제가 가능합니다. Diner's Club 또는 Discover 신용카드는 사용할 수 없습니다.

자세한 내용은 AWS Marketplace 구매자 세금 도움말을 참조하세요.

비용 할당 태그 지정

AWS Marketplace는 구매자가 구매하는 소프트웨어 제품에 대한 비용 할당 태그 지정을 지원합니다. 구매자는 활성화된 비용 할당 태그를 사용하여 AWS Cost Explorer, AWS Cost & Usage Report, AWS Budgets 또는 기타 클라우드 비용 분석 도구를 통해 AWS Marketplace 리소스 사용량을 확인하고 추적할 수 있습니다. AWS Marketplace 비용을 쉽게 범주화하고 추적하려면 비용 할당 태그를 사용하여 비용 할당 보고서에서 리소스 비용을 정리하면 됩니다.

AWS Marketplace의 비용 할당 태그는 다음과 같은 두 가지 소스를 통해 제공됩니다.

- 태그를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 연결된 Amazon Machine Image(AMI) 소프트웨어 제품 비용은 동일한 태그를 상속합니다. 계정의 AWS Billing and Cost Management 콘솔에서 이러한 태그를 비용 할당 태그로 활성화할 수 있습니다. AMI 제품에 비용 할당 태그 사용에 대한 자세한 내용은 AMI 제품의 비용 할당 태그 지정 섹션을 참조하세요.
- AMI, 컨테이너 및 서비스형 소프트웨어(SaaS) 제품에 공급업체에서 제공한 태그가 있을 수 있습니다. 예를 들어 사용자 수를 기준으로 요금을 청구하는 SaaS 제품은 태그를 사용하여 부서별로 사용량을 확인할 수 있습니다. 이러한 태그 사용에 대한 자세한 내용은 공급업체 측정 태그 섹션을 참조하세요.

비용 할당 태그 지정은 과금 정보 및 비용 관리 콘솔에서 태그가 활성화된 시점 이후의 비용만 추적합니다. AWS 계정 소유자, AWS Organizations 관리 계정 소유자 및 적절한 권한이 있는 사용자만 계정의 과금 정보 및 비용 관리 콘솔에 액세스할 수 있습니다. 비용 할당 태그 사용 여부는 청구되는 금액에 영향을 주지 않습니다. 비용 할당 태그 사용 여부는 AWS Marketplace 소프트웨어 제품의 기능에 영향을 주지 않습니다.

EMEA 적격 판매자의 구독은 Cost & Usage Report에 AWS 계약 당사자(Amazon Web Services EMEA SARL) 열이 있습니다.

공급업체 측정 태그

공급업체에서 측정하는 AWS Marketplace 제품(AMI, 컨테이너 및 SaaS 제품 포함)에는 소프트웨어 공급업체가 고객을 위한 추가 서비스로 제공하는 태그가 있을 수 있습니다. 이러한 태그는 공급업체가 제공한 지표 전반의 AWS Marketplace 리소스 사용량을 이해하는 데 도움이 되는 비용 할당 태그입니다. 이러한 태그를 사용하여 AWS Cost Explorer Service, AWS Cost and Usage Report, AWS Budgets 또는 기타 클라우드 비용 분석 도구를 통해 AWS Marketplace 리소스 사용량을 식별하고 추적할 수 있습니다.

구매자가 AWS Marketplace 제품 사용을 시작하고 공급업체가 측정 기록을 AWS Marketplace에 보내면 AWS Billing 콘솔에 태그가 표시됩니다. 구매자가 계약의 선결제 약정에 따라 제품을 사용하는 경우 해당 제품의 사용량 측정 기록을 받을 수 없습니다. 따라서 AWS Billing 콘솔에 공급업체 측정 태그가 없습니다. 구매자가 연결 계정을 관리하는 경우 AWS Billing에서 태그를 보고 활성화하려면 `ModifyBilling` 및 `ViewBilling` 권한이 모두 필요합니다. 자세한 내용은 AWS 결제 사용 설명서의 AWS 결제 작업 정책을 참조하세요.

> **Note**
>
> 공급업체 측정 태그를 활성화하면 비용 및 사용 보고서의 크기가 커질 수 있습니다. 비용 및 사용 보고서는 Amazon S3에 저장됩니다. 따라서 Amazon S3 비용도 증가할 수 있습니다.

모든 적격 AWS Marketplace 제품에 공급업체 측정 태그를 활성화하는 방법

1. AWS Management Console에 로그인한 다음 AWS Billing 콘솔을 엽니다. 왼쪽 탐색 창에서 비용 할당 태그를 선택합니다.
2. AWS에서 생성하는 비용 할당 태그를 선택합니다.
3. `aws:marketplace:isv:`를 검색하여 공급업체 측정 태그를 지원하는 모든 제품의 태그를 찾습니다.
4. 모든 태그의 확인란을 선택하고 활성화를 선택합니다. 공급업체 측정 태그는 24시간 이내에 적용됩니다.

관련 주제

자세한 정보는 다음 주제를 참조하세요.

- AWS Billing 사용 설명서의 비용 할당 태그 사용
- AWS Billing 사용 설명서의 AWS에서 생성하는 비용 할당 태그 활성화

프라이빗 마켓플레이스

프라이빗 마켓플레이스는 비즈니스 사용자, 엔지니어링 팀 같은 AWS 계정의 사용자가 AWS Marketplace에서 조달할 수 있는 제품을 제어합니다. AWS Marketplace를 기반으로 하며, 관리자는 사내 정책에 따라 승인된 독립 소프트웨어 개발 판매 회사(ISV) 및 제품의 큐레이션된 디지털 카탈로그를 생성하고 사용자 지정할 수 있도록 지원합니다. AWS 계정의 사용자는 프라이빗 마켓플레이스에서 승인된 제품을 검색, 구매 및 배포할 수 있으며, 제공되는 모든 제품이 조직의 정책과 표준을 따르도록 관리할 수 있습니다.

프라이빗 마켓플레이스는 다양한 제품 카탈로그와 해당 제품에 대한 세밀한 관리를 제공합니다. AWS Marketplace 를 사용하면 모든 계정을 중앙 집중식으로 관리하고, 계정을 조직 단위 (OU) 로 그룹화하고, 각 OU에 서로 다른 액세스 정책을 적용할 수 있습니다. AWS Organizations 조직 전체, 하나 이상의 OU 또는 조직 내 하나 이상의 계정과 관련된 여러 개의 비공개 마켓플레이스 환경을 만들 수 있으며, 각 계정에는 승인된 제품 세트가 있습니다. 또한 AWS 관리자는 회사 또는 팀의 로고, 메시지 및 색 구성표를 사용하여 각 비공개 마켓플레이스 환경에 회사 브랜딩을 적용할 수 있습니다.

이 섹션에서는 구매자로서 프라이빗 마켓플레이스를 사용하는 방법에 대해 설명합니다. 관리자의 프라이빗 마켓플레이스 관리에 대한 자세한 내용은 프라이빗 마켓플레이스 생성 및 관리 섹션을 참조하세요.

참고

- (비공개 제안을 통해) 공유된 비공개 제품을 프라이빗 마켓플레이스에 추가할 수 있습니다. 자세한 설명은 프라이빗 마켓플레이스에서 비공개 제품 구독 섹션을 참조하세요.
- 프라이빗 마켓플레이스에서 고객에게는 AWS 고객 계약 또는 AWS 서비스 사용과 관련하여 AWS와 맺은 기타 계약에 따라 EULA가 관리되는 모든 제품을 구매할 수 있는 권한이 자동으로 부여됩니다. 고객에게는 이미 기본적으로 이러한 제품을 구매할 수 있는 권한이 있으므로 이러한 제품은 프라이빗 마켓플레이스에서 승인한 제품 목록에 포함되지 않습니다. 고객은 Service Catalog를 사용하여 이러한 제품의 배포를 관리할 수 있습니다.

제품 세부 정보 페이지 보기

사용자는 계정을 관리하는 프라이빗 마켓플레이스에서 허용된 제품만 구독할 수 있습니다. 사용자는 모든 제품의 세부 정보 페이지를 찾아서 볼 수 있지만, 판매자가 프라이빗 마켓플레이스에 추가한 제품만 구독이 활성화됩니다. 제품이 현재 프라이빗 마켓플레이스에 없으면 제품이 AWS Marketplace에서 조달할 수 있도록 승인되지 않았다는 내용의 빨간색 배너가 페이지 상단에 표시됩니다.

소프트웨어 요청이 활성화된 경우 사용자는 제품 세부 정보 페이지에서 요청 생성을 선택할 수 있습니다. 사용자가 요청 생성을 선택하면 관리자에게 제품을 프라이빗 마켓플레이스에서 사용할 수 있도록 하는 요청을 제출합니다. 이 기능에 대한 자세한 내용은 사용자 요청 관리 섹션을 참조하세요.

프라이빗 마켓플레이스에서 제품 구독

프라이빗 마켓플레이스에서 사용자로서 제품을 구독하려면 제품 세부 정보 페이지로 이동하여 계속을 선택합니다. 그러면 제품 구독 페이지로 리디렉션됩니다. 구독 페이지에서 구성을 선택한 다음 구독을 선택할 수 있습니다.

프라이빗 마켓플레이스에서 제품이 승인되지 않은 경우 구독을 사용할 수 없습니다. 페이지 상단의 빨간색 배너는 현재 제품 조달이 승인되지 않음을 나타냅니다. 소프트웨어 요청이 활성화된 경우 요청 생성을 선택하여 관리자에게 제품을 프라이빗 마켓플레이스에 추가하도록 요청하는 요청을 제출할 수 있습니다.

프라이빗 마켓플레이스에서 비공개 제품 구독

일부 제품은 AWS Marketplace에서 공개적으로 찾을 수 없습니다. 이러한 제품은 판매자로부터 비공개 제안을 받은 경우에만 볼 수 있습니다. 하지만 프라이빗 마켓플레이스 관리자가 먼저 프라이빗 마켓플레이스에 제품을 추가한 경우에만 제품을 구독할 수 있습니다. 따라서 비공개 제안을 AWS 계정과 조직의 프라이빗 마켓플레이스 관리자가 포함된 계정에 제시해야 합니다. 사용자와 관리자에게 비공개 제안을 제시한 후에는 프라이빗 마켓플레이스 관리자가 제품을 프라이빗 마켓플레이스에 추가할 수 있습니다. 제품이 승인되면 다른 비공개 제안과 마찬가지로 제품을 구독할 수 있습니다.

프라이빗 마켓플레이스에 제품 추가 요청

사용자는 관리자에게 프라이빗 마켓플레이스에 없는 제품을 추가해 달라고 요청할 수 있습니다. 요청하려면 제품의 세부 정보 페이지로 이동하여 요청 생성을 선택하고 관리자에게 제품을 프라이빗 마켓플레이스에 추가하라는 요청을 입력한 다음 요청을 제출합니다. 요청 상태를 추적하려면 왼쪽 드롭다운 메뉴에서 비 프라이빗 마켓플레이스 요청을 선택합니다.

프라이빗 마켓플레이스 생성 및 관리

비공개 마켓플레이스를 생성하고 관리하려면 관리 계정 또는 프라이빗 마켓플레이스의 위임된 관리자 계정에 로그인해야 합니다. 또한 IAM 정책의 AWS Identity and Access Management (IAM) 권한이 있어야 합니다AWSPrivateMarketplaceAdminFullAccess. 이 정책을 사용자, 그룹 및 역할에 적용하는 자세한 내용은 the section called “프라이빗 마켓플레이스 관리자 생성” 섹션을 참조하세요.

> **Note**
>
> 프라이빗 마켓플레이스 AWS Organizations 통합이 없는 현재 프라이빗 마켓플레이스 고객이라면 AWSPrivateMarketplaceAdminFullAccess IAM 정책이 적용되는 조직의 모든 계정에서 프라이빗 마켓플레이스를 생성하고 관리할 수 있습니다.

이 섹션에는 프라이빗 마켓플레이스 관리자가 AWS Marketplace 웹 사이트를 통해 수행할 수 있는 작업에 대한 내용이 포함되어 있습니다. AWS Marketplace Catalog API를 사용하여 프라이빗 마켓플레이스를 관리할 수도 있습니다. 자세한 내용은 AWS Marketplace Catalog API 참조의 프라이빗 마켓플레이스 작업을 참조하세요.

프라이빗 마켓플레이스 시작하기

프라이빗 마켓플레이스를 시작하려면 AWS 관리 계정에 로그인하고 Private Marketplace로 이동한 후 다음 사전 요구 사항을 활성화해야 합니다.

- 신뢰할 수 있는 액세스 — 신뢰할 수 있는 액세스를 활성화해야 합니다. 그러면 조직의 관리 계정이 서비스에 대한 AWS Organizations 데이터 액세스를 제공하거나 취소할 수 있습니다. AWS Organizations AWS 프라이빗 마켓플레이스가 프라이빗 AWS Organizations 마켓플레이스와 통합되고 프라이빗 마켓플레이스를 조직의 신뢰할 수 있는 서비스로 지정하려면 신뢰할 수 있는 액세스를 활성화하는 것이 중요합니다.
- 서비스 연결 역할 — 프라이빗 마켓플레이스 서비스 연결 역할을 활성화해야 합니다. 이 역할은 관리 계정에 있으며, 프라이빗 마켓플레이스에서 사용자를 대신하여 프라이빗 마켓플레이스 리소스를 설명하고 AWS Organizations 업데이트하는 데 필요한 모든 권한을 포함합니다. 서비스 연결 역할에 대한 자세한 내용은 에서 역할을 사용하여 Private Marketplace 구성을 참조하십시오. AWS Marketplace

> **Note**
>
> 현재 프라이빗 마켓플레이스 고객은 Private Marketplace 관리자 페이지로 이동한 다음 설정을 선택하여 프라이빗 마켓플레이스에 대한 설정을 활성화할 수 있습니다. 신뢰할 수 있는 액세스를 AWS Organizations 활성화하고 서비스 연결 역할을 생성하면 OU를 프라이빗 마켓플레이스 경험에 연결하고 위임된 관리자를 등록하는 등의 기능을 활용할 수 있습니다. 활성화된 경우 관리 계정 및 위임된 관리자 계정만이 마켓플레이스 경험을 생성 및 관리할 수 있으며, 기존 리소스는 관리 계정으로 이전되고 위임된 관리자와만 공유됩니다. 신뢰할 수 있는 액세스를 비활성화하면 조직의 프라이빗 마켓플레이스 거버넌스가 제거됩니다. 프라이빗 마켓플레이스에

는 계정 그룹이 표시되지 않습니다. 다양한 수준에서 조직의 거버넌스를 보려면 조직 구조 페이지를 사용하세요. 질문이나 지원이 필요하면 문의해 주세요.

프라이빗 마켓플레이스 관리

왼쪽 창의 설정에 있는 Private Marketplace 관리자 페이지에서 비공개 마켓플레이스를 관리할 수 있습니다. 관리 계정 관리자와 위임된 관리자는 이 페이지에서 기본 프라이빗 마켓플레이스 및 라이브 경험 수를 비롯한 프라이빗 마켓플레이스 세부 정보를 볼 수 있습니다.

관리 계정 관리자는 이 페이지를 사용하여 다음 설정을 관리할 수도 있습니다.

위임된 관리자

관리 계정 관리자는 위임 관리자라고 하는 지정된 멤버 계정에 프라이빗 마켓플레이스 관리 권한을 위임할 수 있습니다. 계정을 프라이빗 마켓플레이스의 위임 관리자로 등록하려면 관리 계정 관리자가 신뢰할 수 있는 액세스와 서비스 연결 역할이 활성화되어 있는지 확인하고, 새 관리자 등록을 선택하고, 12자리 AWS 계정 번호를 입력한 다음 제출을 선택해야 합니다.

관리 계정 및 위임된 관리자 계정은 경험 생성, 브랜드 설정 업데이트, 대상 연결 또는 연결 해제, 제품 추가 또는 제거, 보류 중인 요청 승인 또는 거부와 같은 비공개 마켓플레이스 관리 작업을 수행할 수 있습니다.

신뢰할 수 있는 액세스 및 서비스 연계 역할

관리 계정 관리자는 프라이빗 마켓플레이스에서 다음 기능을 활성화할 수 있습니다.

> **Note**
>
> 현재 프라이빗 마켓플레이스 고객은 Private Marketplace 관리자 페이지로 이동한 다음 설정을 선택하여 프라이빗 마켓플레이스에 대한 설정을 활성화할 수 있습니다. 신뢰할 수 있는 액세스를 AWS Organizations 활성화하고 서비스 연결 역할을 생성하면 OU를 프라이빗 마켓플레이스 경험에 연결하고 위임된 관리자를 등록하는 등의 기능을 활용할 수 있습니다. 활성화된 경우 관리 계정 및 위임된 관리자 계정만이 마켓플레이스 경험을 생성 및 관리할 수 있으며, 기존 리소스는 관리 계정으로 이전되고 위임된 관리자와만 공유됩니다. 신뢰할 수 있는 액세스를 비활성화하면 조직의 프라이빗 마켓플레이스 거버넌스가 제거됩니다. 프라이빗 마켓플레이스에는 계정 그룹이 표시되지 않습니다. 다양한 수준에서 조직의 거버넌스를 보려면 조직 구조 페이지를 사용하세요. 질문이나 지원이 필요하면 문의해 주세요.

- 신뢰할 수 있는 액세스 — 조직의 관리 계정이 서비스에 대한 AWS Organizations AWS Organizations 데이터 액세스를 제공하거나 취소할 수 있도록 하려면 신뢰할 수 있는 액세스를 활성화해야 합니다. AWS 프라이빗 마켓플레이스가 프라이빗 AWS Organizations 마켓플레이스와 통합되고 프라이빗 마켓플레이스를 조직의 신뢰할 수 있는 서비스로 지정하려면 신뢰할 수 있는 액세스를 활성화하는 것이 중요합니다.
- 서비스 연결 역할 — 프라이빗 마켓플레이스 서비스 연결 역할을 활성화해야 합니다. 이 역할은 관리 계정에 있으며, 프라이빗 마켓플레이스에서 사용자를 대신하여 프라이빗 마켓플레이스 리소스를 설명하고 AWS Organizations 업데이트하는 데 필요한 모든 권한을 포함합니다. 서비스 연결 역할에 대한 자세한 내용은 에서 역할을 사용하여 Private Marketplace 구성을 참조하십시오. AWS Marketplace

프라이빗 마켓플레이스 경험 생성

프라이빗 마켓플레이스는 하나 이상의 프라이빗 마켓플레이스 경험으로 구성됩니다. 경험은 전체 조직, 하나 이상의 OU 또는 조직 내 하나 이상의 계정과 연결될 수 있습니다. 조직의 AWS 계정 구성원이 아닌 경우 계정 하나에 비공개 마켓플레이스 경험이 하나 연결되어 있는 것입니다. 프라이빗 마켓플레이스를 생성하려면 프라이빗 마켓플레이스로 이동하고, 왼쪽에서 경험 페이지를 선택하고, 경험 생성을 선택합니다.

> **Note**
>
> 에서 프라이빗 마켓플레이스를 AWS Organizations 사용하려면 조직의 모든 기능을 활성화해야 합니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.
>
> 조직의 AWS 계정 구성원이 아닌 경우 프라이빗 마켓플레이스를 사용하기 위한 사전 단계가 필요하지 않습니다.

프라이빗 마켓플레이스 경험은 승인된 제품이나 브랜딩 요소가 없는 상태로 생성되며, 조직 내 계정과 연결되지 않습니다. 기본적으로 라이브는 아닙니다. 다음 주제에서는 프라이빗 마켓플레이스 경험을 활용하는 방법을 설명합니다.

프라이빗 마켓플레이스에 제품 추가

프라이빗 마켓플레이스 경험에 제품을 추가하는 방법

1. 프라이빗 마켓플레이스 관리자 페이지의 왼쪽 탐색 창에서 경험을 선택합니다. 그런 다음 제품 탭에서 모든 AWS Marketplace 제품을 선택합니다. 제품 이름 또는 판매자 이름으로 검색할 수 있습니다.
2. Private Marketplace에 추가할 제품 옆에 있는 확인란과 Add to Private Marketplace(Private Marketplace에 추가)를 차례대로 선택합니다.

> **Note**
>
> 빨간색 배너에서 프라이빗 마켓플레이스에 추가 버튼을 선택하여 제품 세부 정보 페이지에서 직접 제품을 추가할 수도 있습니다. 제품 세부 정보 페이지에 빨간색 배너가 없으면 해당 제품이 이미 프라이빗 마켓플레이스에 있는 것입니다.

왼쪽 탐색 창에서 제품 대량 추가/제거를 선택하여 한 번에 여러 제품을 여러 경험에 추가할 수도 있습니다.

프라이빗 마켓플레이스 경험에서 제품 확인

프라이빗 마켓플레이스 경험에서 제품이 승인되었는지 확인하는 방법

1. 프라이빗 마켓플레이스 관리자 페이지의 왼쪽 탐색 창에서 경험을 선택합니다.
2. 승인된 제품을 선택합니다. 승인된 모든 제품이 승인 목록에 표시됩니다.

> **Note**
>
> 편집 중인 경험과 연결된 계정을 사용 중이고 경험이 활성화된 경우 AWS Marketplace 콘솔(https://console.aws.amazon.com/marketplace)에서 직접 제품을 볼 수도 있습니다. 프라이빗 마켓플레이스에 있는 제품인 경우 검색 결과의 모든 제품에 조달 승인 배지가 표시됩니다.

프라이빗 마켓플레이스 경험 사용자 지정

경험은 제품 및 관련 브랜드의 하위 집합으로, 관련 잠재고객이 한 명 이상일 수 있습니다. 경험이 조직과 연계되어 있는 경우 단일 프라이빗 마켓플레이스 경험이 전체 조직을 관리하거나 조직 내 하나 이상의 계정 또는 조직 단위를 관리할 수 있습니다.

왼쪽 창의 경험 아래에 있는 Private Marketplace 관리자 페이지에서 경험 설정을 관리할 수 있습니다. 이 페이지를 사용하여 모든 활성 및 보관된 경험을 보고 관리하고 프라이빗 마켓플레이스를 위한 새로운 경험을 만들 수 있습니다. 각 경험에 대해 로고를 추가하고, 제목을 추가하고, 조직의 색 구성표를 사용하도록 사용자 인터페이스를 사용자 지정할 수 있습니다.

잠재고객 관리

잠재고객은 프라이빗 마켓플레이스 경험과 연결할 수 있는 조직 또는 OU (조직 구성 단위) 또는 계정 그룹입니다. 왼쪽 창의 경험 아래에 있는 Private Marketplace 관리자 페이지에서 대상을 만들 수 있습니다.

한 명 이상의 잠재고객을 경험에 연결할 수 있습니다. 잠재고객을 연결하거나 연결 해제하면 자녀 OU 및 계정의 관리 환경이 변경될 수 있습니다. 조직 구조 페이지를 사용하여 연결의 영향을 받는 계정 및 OU를 확인할 수 있습니다. 신뢰할 수 있는 액세스를 비활성화하면 대상 그룹이 분리되고 모든 거버넌스가 제거됩니다.

> **Note**
>
> 프라이빗 마켓플레이스에서 조직의 AWS Organizations 계층 구조를 확인하고 거버넌스를 관리할 수 있습니다. 조직 단위 수준에서 프라이빗 마켓플레이스를 관리하고 위임된 관리자를 등록하려면 설정 페이지에서 신뢰할 수 있는 액세스 및 서비스 연결 역할을 활성화하세요. 질문이나 지원이 필요한 경우 당사로 문의하세요.

프라이빗 마켓플레이스 구성

경험의 제품 목록, 마켓플레이스의 브랜딩 설정, 연결된 계정 그룹에 만족하면 프라이빗 마켓플레이스를 라이브로 전환할 수 있습니다. AWSPrivate Marketplace 관리자 페이지의 왼쪽 탐색 창에서 경험을 선택한 다음 활성화하려는 경험을 선택합니다. 설정 탭에서 프라이빗 마켓플레이스 상태를 라이브(활성화됨)와 라이브 아님(비활성화됨) 간에 전환할 수 있습니다.

사용자가 소프트웨어 요청을 사용하여 소프트웨어 요청을 제출하도록 허용할 수도 있습니다. 소프트웨어 요청이 켬(활성화됨)이면 최종 사용자는 제품 세부 정보 페이지에서 요청 생성을 선택하여 프라이

빗 마켓플레이스에서 제품을 판매할 수 있게 해 달라는 요청을 관리자에게 제출할 수 있습니다. 소프트웨어 요청은 기본적으로 활성화되며, 프라이빗 마켓플레이스가 활성화된 경우에만 설정을 수정할 수 있습니다.

프라이빗 마켓플레이스가 활성화되면 최종 사용자는 판매자가 승인한 제품만 구매할 수 있습니다. Private Marketplace가 비활성화되어도 제품 목록은 그대로 유지됩니다. 하지만 프라이빗 마켓플레이스를 비활성화하면 AWS Organizations 조직 내 사용자에게 적용되는 제한이 사라집니다. 따라서 AWS Marketplace에 공개된 모든 제품을 구독할 수 있게 됩니다.

프라이빗 마켓플레이스를 라이브로 전환해도 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 실행 중인 활성 Amazon Machine Image(AMI)는 중단되지 않습니다. 모범 사례는 현재 조직 전체에서 사용 중인 모든 AWS Marketplace 제품을 프라이빗 마켓플레이스에 포함하는 것입니다. 프라이빗 마켓플레이스를 라이브로 전환하기 전에, 승인되지 않은 제품 사용을 중단할 계획을 세우는 것도 모범 사례입니다. 프라이빗 마켓플레이스가 라이브로 전환되면 모든 신규 구독 또는 갱신은 프라이빗 마켓플레이스 카탈로그의 승인된 제품을 통해 관리됩니다.

비공개 제품 작업

일부 제품은 AWS Marketplace에서 공개적으로 찾을 수 없습니다. 이러한 제품은 판매자로부터 비공개 제안을 받은 경우에만 볼 수 있습니다. 판매자의 비공개 제안에는 제품 링크가 포함되어 있습니다. 페이지 상단의 배너에서 제품을 프라이빗 마켓플레이스에 추가할 수 있습니다.

> **Note**
>
> 조직의 다른 계정에서 비공개 제품을 구독하려는 경우 판매자는 프라이빗 마켓플레이스에 제품을 추가하는 데 사용할 AWS 계정과 제품을 구독하는 데 사용할 사용자 계정을 모두 비공개 제안에 포함해야 합니다.

비공개 마켓플레이스에서 비공개 제품을 제거하려면 AWS Marketplace 지원에 문의해야 합니다.

사용자 요청 관리

사용자가 소프트웨어 요청 기능을 사용하여 프라이빗 마켓플레이스 카탈로그에 제품을 추가해 달라는 요청을 제출할 수 있도록 허용할 수 있습니다. 이렇게 하려면 프라이빗 마켓플레이스의 관리자 페이지로 이동하고, 왼쪽 탐색 창에서 경험을 선택하고, 관리하려는 경험을 선택합니다. 제품 탭에서 보류 중인 요청을 선택합니다. 여기에서 프라이빗 마켓플레이스 카탈로그에 제품을 추가해 달라는 사용자의 요청을 검토할 수 있습니다.

먼저 요청된 각 제품 이름 옆에 있는 확인란을 선택한 다음 프라이빗 마켓플레이스에 추가를 선택하여 이 페이지에서 요청된 제품을 원하는 수만큼 추가할 수 있습니다. 마찬가지로 거부를 선택하여 하나 이상의 선택된 요청을 거부할 수도 있습니다. 제품(또는 제품의 소프트웨어 요청)에 대한 자세한 내용을 보려면 해당 요청의 세부 정보 열에서 세부 정보 보기를 선택합니다.

제품 요청을 거부하는 경우 사유를 추가하고 이 제품에 대한 향후 요청을 금지(차단)할 수 있습니다. 제품을 차단해도 판매자는 프라이빗 마켓플레이스에 제품을 추가할 수 있고, 사용자는 제품을 요청할 수는 없습니다.

프라이빗 마켓플레이스 경험 보관 및 재활성화

프라이빗 마켓플레이스 경험을 보관하여 제거할 수 있습니다. 보관된 경험을 업데이트하거나 조직의 계정을 관리하는 데 사용할 수 없습니다. 보관된 경험과 관련된 잠재고객이 있는 경우 이들을 다른 경험과 연결할 수 있습니다. 나중에 언제든지 보관된 경험을 다시 활성화할 수 있습니다. 관리 계정 관리자 또는 위임된 관리자는 경험을 보관하고 다시 활성화할 수 있는 권한이 있습니다.

> **Note**
>
> 경험을 보관하기 전에 반드시 비활성화해야 합니다. 경험 비활성화에 대한 자세한 내용은 프라이빗 마켓플레이스 구성을 참조하세요.
> 프라이빗 마켓플레이스 AWS Organizations 통합이 없는 현재 프라이빗 마켓플레이스 고객인 경우 경험을 만든 계정의 관리자는 경험을 보관하고 다시 활성화할 수 있는 권한을 갖습니다.

하나 이상의 프라이빗 마켓플레이스 경험을 보관하는 방법

1. 프라이빗 마켓플레이스 관리자 페이지의 왼쪽 탐색 창에서 경험을 선택합니다.
2. 활성 경험 탭에서 하나 이상의 경험을 선택합니다.
3. 경험 보관을 선택합니다.

> **Note**
>
> 경험 중 하나 이상이 라이브 상태인 경우 경험을 오프라인으로 전환을 선택하여 경험을 오프라인으로 전환해야 합니다.

4. 텍스트 상자에 **`confirm`**(모두 소문자)을 입력하여 경험을 보관하려는 것이 맞는다고 확인합니다.
5. Archive(아카이브)를 선택합니다.

> **Note**
>
> 경험을 선택하고 설정 탭의 관리자 모드에서 경험 보관을 선택한 다음, 저장을 선택하여 경험을 보관할 수도 있습니다.

하나 이상의 프라이빗 마켓플레이스 경험을 재활성화하는 방법

1. 프라이빗 마켓플레이스 관리자 페이지의 왼쪽 탐색 창에서 경험을 선택합니다.
2. 보관된 경험 탭에서 하나 이상의 경험을 선택합니다.
3. 다시 활성화를 선택합니다.
4. 텍스트 상자에 **`confirm`**을 입력하여 경험을 다시 활성화하려는 것이 맞는다고 확인합니다.
5. 다시 활성화를 선택합니다.

> **Note**
>
> 경험을 선택하고 설정 탭의 관리자 모드에서 경험 다시 활성화를 선택한 다음, 저장을 선택하여 경험을 다시 활성화할 수도 있습니다.

비공개 제안

AWS Marketplace 판매자 비공개 제안 기능을 사용하면 판매자로부터 공개적으로 이용할 수 없는 제품 요금 및 EULA 조건을 얻을 수 있습니다. 판매자와 요금 및 조건을 협상하면, 판매자는 사용자가 지정하는 AWS 계정에 비공개 제안을 생성합니다. 비공개 제안을 수락하고 협상된 요금 및 이용 약관을 받기 시작합니다.

비공개 제안마다 계정에 고유하게 제공된 요금 및 라이선스 약관이 있습니다. 제품 판매자는 비공개 제안을 제시하며, 제안에는 설정된 만료 날짜가 있습니다. 만료 날짜까지 비공개 제안을 수락하지 않으면 비공개 제안 대상인 제품의 유형에 따라 해당 제품의 공개 제안으로 자동으로 이동하거나 제품 구독이 해지됩니다.

AWS Organizations에서 통합 결제 기능을 사용하는 경우 조직의 관리 계정 또는 멤버 계정에서 비공개 제안을 수락할 수 있습니다. 관리 계정에서 수락하면 조직의 모든 멤버 계정과 비공개 제안을 공유할 수 있습니다. 요금 혜택을 받으려면 이전에 제품을 구독한 멤버 계정도 새 비공개 제안을 수락해야 합니다. 또는 AMI 및 컨테이너 제품의 경우 AWS License Manager를 사용하여 관리 계정의 라이선스를 멤버 계정과 공유할 수 있습니다. 이전에 제품을 구독하지 않은 멤버 계정은 새 비공개 제안을 수락해야만 제품을 배포할 수 있습니다.

통합 결제에 대한 자세한 내용는 AWS Billing 사용 설명서의 조직에 대한 통합 결제를 참조하세요. 다음은 비공개 제안을 사용하기 시작할 때 유의야 할 주요 사항입니다.

- AWS Marketplace 구매자는 비공개 제안에 타사 파이낸싱 서비스를 이용할 수 있습니다. 자세한 내용은 이제 AWS Marketplace에서 고객 파이낸싱 이용 가능을 참조하세요.
- 비공개 제안을 사용하여 구매한 소프트웨어 제품은 차이가 없습니다. 비공개 제안을 사용하여 구매한 소프트웨어의 사용 방식은 비공개 제안 없이 소프트웨어를 구매하는 경우와 동일합니다.
- 비공개 제안을 사용하여 구매한 제품 구독은 월간 청구서에서 다른 AWS Marketplace 제품과 똑같이 표시됩니다. 세부 청구 정보를 사용해 각 AWS Marketplace 구매 제품의 사용량을 확인할 수 있습니다. 각 비공개 제안에는 각 사용량 유형에 따른 항목이 있습니다.
- 비공개 제안 구독 시 새로운 소프트웨어 인스턴스를 시작할 필요는 없습니다. 비공개 제안을 수락하면 비공개 제안 요금에 따라 사용 요금이 바뀝니다. 구독 제품이 1-Click Launch를 제공하는 경우 고객은 새로운 소프트웨어 인스턴스를 배포할 수 있습니다. 제품에서 1-Click Launch가 기본값으로 설정된 경우 고객은 새로운 인스턴스를 시작하지 않아도 비공개 제안을 수락할 수 있습니다. 새로운 인스턴스를 배포하지 않고 시작하려면 실행 페이지에서 Manual Launch(수동 시작)를 선택하십시오. Amazon Elastic Compute Cloud 콘솔을 사용하여 다른 AWS Marketplace 제품에 하는 것처럼 인스턴스를 추가로 배포할 수 있습니다.

- 판매자가 구매자에게 비공개 제안을 제시하면 구매자는 판매자가 비공개 제안에 포함한 계정을 확인하라는 메시지를 수신합니다. 그러면 비공개 제안이 해당하는 소프트웨어 구매자의 계정으로 연결됩니다. 소프트웨어 판매자는 구매자가 지정하는 계정으로 비공개 제안을 생성합니다. 각 비공개 제안은 최대 25개 계정까지 가능합니다.
- 구매자가 비공개 제안을 수락하면 구매자와 판매자 간의 계약(agreement 또는 contract 또는 구독)이 성립됩니다.
- 판매자는 SaaS 계약 또는 소비 제품이 포함된 SaaS 계약의 구매를 업그레이드하거나 갱신하도록 제안할 수 있습니다. 예를 들어 판매자는 새로운 권한을 부여하거나, 요금 할인을 적용하거나, 결제 일정을 조정하거나, 표준화된 라이선스 조건을 사용하도록 최종 사용자 라이선스 계약(EULA)을 변경하기 위해 새 비공개 제안을 생성할 수 있습니다.

  이러한 갱신 또는 업그레이드는 구매자가 수락한 원래 비공개 제안의 변경 사항이며, 구매자는 이를 수락하는 데에도 동일한 프로세스를 사용합니다. 구매자가 새 업그레이드 또는 갱신 비공개 제안을 수락하면 소프트웨어 서비스의 중단 없이 새 계약 조건이 즉시 적용됩니다. 이전 조건 또는 예정된 남은 결제 항목이 취소되고 이 새 계약의 조건으로 대체됩니다.
- 연간 소프트웨어 구독은 모두 AWS Marketplace의 사용자 소프트웨어 아래에서 살펴볼 수 있습니다. 통합 결제를 위해 AWS Organizations를 사용하여 한 계정에서 연간 구독을 구매한 경우, 연결된 계정 패밀리 전체에서 이 연간 구독을 공유합니다. 구매한 계정에 실행 중인 인스턴스가 전혀 없으면 연간 구독은 해당 소프트웨어를 실행하는 다른 연결 계정의 사용량에 포함됩니다. 연간 구독에 대한 자세한 내용은 the section called “AMI 구독” 단원을 참조하십시오.
- 만료된 비공개 제안은 구독할 수 없습니다. 하지만 판매자에게 문의해 볼 수는 있습니다. 판매자에게 현재 제안의 만료 날짜를 미래의 날짜로 변경하거나 새 비공개 제안을 생성해 달라고 요청하세요.

비공개 제안 대상인 제품 유형

다음 제품 유형에 대해 비공개 제안을 받을 수 있습니다.

제안 유형	Description
데이터 제품	자세한 내용은 AWS Data Exchange 사용 설명서의 비공개 제안 수락을 참조하세요.
SaaS 계약	Software as a Service(SaaS) 계약에서는 SaaS 제품의 예상 사용량에 대해 선결제 금액을 약정하거나 판매자와 유연한 결제 일정을 협상할 수 있습니다. 계약 기간은 1개월, 1년, 2년 또는 3년

제안 유형	Description
	기간이며 월 단위로 최대 60개월까지 사용자 지정 기간을 선택할 수도 있습니다. 선결제를 약정한 경우 제품 소프트웨어 사용 요금이 미리 청구됩니다. 판매자가 유연한 결제 일정을 제공하는 경우에는 비공개 제안에 나열된 금액이 결제 예정일에 청구됩니다. 계약된 사용량을 초과하는 사용량에 대해서는 협상된 사용량에 따른 요금을 적용한다는 조항을 판매자가 포함할 수도 있습니다.
SaaS 구독	SaaS 구독의 경우, 제품 사용 가격에 동의합니다. 판매자가 사용량을 추적하고 AWS Marketplace에 보고합니다. 사용량에 대해 요금이 청구됩니다.
AMI 시간별 구독	Amazon Machine Image(AMI) 시간별 구독의 경우, AMI 사용에 대한 시간당 요금을 협상합니다. 이때 가장 가까운 시간으로 올림됩니다.

제안 유형	Description
AMI 연간 시간당 요금	AMI 연간 시간당 요금을 사용하면 인스턴스 유형별로 시간당 요금과 장기 요금을 협상할 수 있습니다. 장기 요금은 비공개 제안에 적용되며, 기간은 1일~3년입니다. 판매자가 유연한 결제 일정이 적용되지 않는 비공개 제안을 생성하는 경우 비공개 제안에서 결정된 시간당 요금으로 Amazon EC2 인스턴스를 실행할 수 있으며, 원한다면 비공개 제안에 책정된 장기 요금으로 계약 기간 동안 선결제 약정을 구매할 수 있습니다. 판매자가 유연한 결제 일정이 적용되는 비공개 제안을 생성하는 경우 사용량에 관계없이 비공개 제안에 표시된 금액이 결제 예정일에 청구됩니다. 이 유형의 비공개 제안에서 판매자는 시간당 요금 없이 실행할 수 있는 여러 Amazon EC2 인스턴스를 인스턴스 유형별로 포함시킬 수 있습니다. 계약에 포함된 용량을 초과하는 사용량에 대해서는 비공개 제안에 책정된 시간당 요금이 청구됩니다.
AMI 계약	AMI 계약의 경우 계약 요금과 계약 기간을 협상으로 정하며, 계약 기간은 1~60개월입니다. 판매자가 유연한 결제 일정이 적용되지 않는 비공개 제안을 생성하는 경우 계약에 동의하는 순간, 비공개 제안에 책정된 가격 및 옵션에 따라 계약을 구성할 수 있습니다. 판매자가 유연한 결제 일정이 적용되는 비공개 제안을 생성하는 경우 비공개 제안에 표시된 금액이 결제 예정일에 청구됩니다. 이 유형의 비공개 제안에서는 판매자가 비공개 제안의 계약을 구성하며 계약이 체결된 이후에는 계약을 구성할 수 없습니다.

제안 유형	Description
컨테이너 제품	컨테이너 제품의 경우 구매하는 제품에 맞는 포드, 작업 또는 사용자 지정 단위별로 사용하는 컨테이너 제품의 시간당 또는 연간 요금을 협상합니다. 컨테이너 제품 비공개 제안은 AMI 제품 비공개 제안과 일치합니다.
기계 학습 제품	지정된 일수 동안 고정 선결제 요금이 적용되는 비공개 제안도 있습니다. 계약이 종료된 후에도 계속 실행되는 인스턴스에 대해 판매자가 비공개 제안에서 설정한 시간당 요금이 청구됩니다.
전문 서비스	모든 전문 서비스 제안은 비공개 제안입니다. 구매자와 협의하여 비공개 제안을 생성해야 합니다. 자세한 정보는 전문 서비스 제품 섹션을 참조하십시오.

비공개 제안 수락 준비

일반적인 비공개 제안을 협상할 때, 구매자는 제3자 파이낸싱을 이용하는 경우를 제외하고 제안 수락 시 제안 금액 전체를 지불합니다. 제3자 파이낸싱을 이용하는 경우 금융사가 구매자 대신 계약금을 지불하고 합의된 결제 일정에 따라 구매자에게 인보이스를 발행합니다. 비공개 제안을 수락하기 전에 회사의 결제 구조, AWS 결제에 대한 지불 방법, 세금 설정을 확인합니다.

AWS Billing and Cost Management 기본 설정 확인

과금 정보 및 비용 관리 서비스는 AWS 청구서를 결제하고 사용량을 모니터링하고 비용 예산을 책정하는 데 사용되는 서비스입니다. AWS Organizations의 통합 결제 기능을 사용하면 여러 계정 또는 여러 Amazon Internet Services Pvt. Ltd(AISPL) 계정의 청구 및 결제를 통합할 수 있습니다. AWS Organizations의 모든 조직에는 모든 멤버 계정의 비용을 지불하는 관리 계정이 하나씩 있습니다. 관리 계정을 지급인 계정이라고 하며, 멤버 계정을 연결된 계정이라고 합니다. 비공개 제안을 협상하기 전에 회사의 AWS 청구서 지불 방식과 비공개 제안을 받는 AWS 계정을 확인합니다.

결제 방법 확인

비공개 제안을 수락하기 전에 해당 결제 방법이 비공개 제안의 전체 비용 지불을 지원하는지 확인합니다. 결제 방법을 확인하려면 https://console.aws.amazon.com/billing/에서 과금 정보 및 비용 관리 콘솔을 엽니다.

세금 설정 확인

회사가 세금 면제를 받을 자격이 있는 경우, 세금 설정을 확인합니다. 세금 설정을 보거나 수정하려면 AWS Management Console에 로그인하고 계정 설정에서 세금 설정을 봅니다. 세금 등록에 대한 자세한 내용은 AWS 계정의 세금 등록 번호 또는 기업의 법적 주소를 추가하거나 업데이트하는 방법은 무엇입니까?를 참조하십시오.

비공개 제안 확인 및 구독

다음 방법 중 하나로 비공개 제안을 볼 수 있습니다.

주제

- 비공개 제안 목록에서 비공개 제안을 살펴보고 구독하기
- 판매자가 제공한 링크를 통해 비공개 제안을 살펴보고 구독하기
- 제품 페이지에서 비공개 제안을 살펴보고 구독하기

비공개 제안 목록에서 비공개 제안을 살펴보고 구독하기

AWS 계정에 제시된 비공개 제안 목록에서 비공개 제안을 살펴보고 구독하는 방법

1. AWS Marketplace 콘솔에 로그인합니다.
2. 비공개 제안 페이지로 이동합니다.
3. 비공개 제안 페이지의 이용 가능한 오퍼 탭에서 관심 있는 제안의 제안 ID를 선택합니다.
4. 비공개 제안을 살펴보고 구독합니다.

판매자가 제공한 링크를 통해 비공개 제안을 살펴보고 구독하기

판매자가 제공한 링크를 통해 비공개 제안을 살펴보고 구독하는 방법

1. AWS Marketplace 콘솔에 로그인합니다.

2. 판매자가 보낸 링크를 따라 비공개 제안에 직접 액세스합니다.

> **Note**
>
> 올바른 계정에 로그인하지 않고 이 링크를 따라가면 Page not found(404) 오류가 발생합니다.
> 자세한 내용은 비공개 제안을 보기 위해 제안 ID를 클릭하면 Page not found(404) 오류가 발생합니다. 섹션을 참조하세요.

3. 비공개 제안을 살펴보고 구독합니다.

제품 페이지에서 비공개 제안을 살펴보고 구독하기

제품 페이지에서 비공개 제안을 살펴보고 구독하는 방법

1. AWS Marketplace 콘솔에 로그인합니다.
2. 제품의 제품 페이지로 이동합니다.
3. 비공개 제안, 제안 ID, 제안 만료 정보를 보여주는 배너가 페이지 맨 위에 표시됩니다.

> **Note**
>
> 미래 날짜의 비공개 제안은 조기 갱신으로 표시됩니다. 자세한 내용은 the section called "미래 날짜의 계약 관련 작업" 섹션을 참조하세요.

4. 제안 ID를 선택합니다.
5. 비공개 제안을 살펴보고 구독합니다.

> **Note**
>
> 해당 제품에 대한 비공개 제안이 둘 이상인 경우, 각 제안이 Offer name(제안 이름) 아래에 표시됩니다. 해당 제품과 체결한 유효 계약이 있는 경우 해당 제안 옆에 사용 중 아이콘이 표시됩니다.

비공개 제안 문제 해결

AWS Marketplace에서 비공개 제안을 작업하는 동안 HTTP 상태 코드 404(Not Found) 또는 이와 유사한 문제가 발생하면 이 섹션의 주제를 참조하세요.

문제

- 비공개 제안을 보기 위해 제안 ID를 클릭하면 Page not found(404) 오류가 발생합니다.
- 어떤 방법으로도 문제가 해결되지 않습니다.

비공개 제안을 보기 위해 제안 ID를 클릭하면 Page not found(404) 오류가 발생합니다.

- 올바른 AWS 계정에 로그인했는지 확인하세요. 판매자가 비공개 제안을 특정 AWS 계정 ID에 제시합니다.
- AWS Marketplace 콘솔의 비공개 제안 아래에 해당 제안이 있는지 확인하세요. 비공개 제안에서 해당 제안을 찾을 수 없으면 판매자가 제안을 다른 AWS 계정 ID에 제시한 것일 수 있습니다. 판매자에게 문의하여 제안이 제시된 AWS 계정 ID를 확인하세요.
- AWS Marketplace 콘솔의 비공개 제안 아래에 있는 수락된 제안 및 만료된 제안 탭을 확인하여 비공개 제안이 만료되지 않았는지 확인하세요. 제안이 만료된 경우 판매자와 협의하여 제안의 만료 날짜를 수정하거나 계정에 새 제안을 제시하세요.
- 비공개 제안을 볼 수 있도록 계정 ID가 허용 목록에 있는지 확인하세요. 일부 ISV는 제한된 목록을 사용합니다. ISV에 문의하여 제품을 볼 수 있도록 계정을 허용 목록에 추가했는지 확인하세요. 제한된 AMI 제품 목록에는 허용 목록이 필요합니다. AWS 조직에 소속되어 있는데 판매자가 관리 계정에 제안을 제시하는 경우 제품을 구독하려면 연결된 계정을 허용 목록에 추가해야 합니다. 그렇지 않으면 허용 목록에 없는 구매자의 연결된 계정에서 제안을 보려고 하면 Page not found(404) 오류가 발생합니다.
- 제안을 확인해야 하는 경우 AWS 관리자에게 문의하여 `aws-marketplace:ViewSubscriptions` IAM 권한이 있는지 확인하세요. AWS Marketplace 보안에 대한 자세한 내용은 AWS Marketplace 보안 섹션을 참조하세요.
- 프라이빗 마켓플레이스를 사용하고 있는지 확인하세요.
  - 제품이 프라이빗 마켓플레이스의 허용 목록에 있는지 확인하세요(해당하는 경우). 그래야만 제품을 구매할 수 있습니다. 잘 모르겠으면 시스템 관리자에게 문의하여 확인하세요.

어떤 방법으로도 문제가 해결되지 않습니다.

어떤 방법으로도 HTTP 상태 코드 404(Not Found) 오류가 해결되지 않으면 브라우저에서 다음 작업을 시도합니다.

- 캐시를 지웁니다.
- 쿠키를 삭제합니다.
- 로그아웃했다가 다시 로그인합니다.
- 시크릿 모드 또는 프라이빗 검색 모드를 사용합니다.
- 다른 브라우저를 사용해 보세요. Internet Explorer는 권장하지 않습니다.

문제 해결 방법을 모두 시도했지만 여전히 Page not found 오류가 발생하는 경우 <mpcustdesk@amazon.com>으로 이메일 메시지를 보내 도움을 받으세요.

AWS Marketplace의 비공개 제안 페이지

AWS Marketplace의 비공개 제안 페이지에는 비공개 및 공개 제품의 AWS 계정에 제시된 모든 비공개 제안이 표시됩니다. 각 제품에 제공되는 모든 제안이 표시됩니다. 제품마다 하나의 제안을 수락할 수 있습니다.

비공개 제안 페이지 이해하기

AWS Marketplace 콘솔에 로그인하고 비공개 제안으로 이동하면 비공개 제안 페이지를 볼 수 있습니다. 비공개 제안 페이지에는 제안 ID, 제품, 등록 판매자(ISV 또는 채널 파트너), 게시자, 유효한 계약(해당하는 경우), 제안 만료일을 포함하여 AWS 계정에 제시된 비공개 제안이 표시됩니다. 관심 있는 제안의 제안 ID를 선택하면 제안 세부 정보를 살펴보고 비공개 제안을 구독할 수 있습니다.

비공개 제안 페이지에는 다음과 같은 정보가 있습니다.

- 이용 가능한 오퍼 탭에는 구매자의 계정에 제시된 비공개 제안 중에서 수락할 수 있는 비공개 제안이 표시됩니다. 이 탭의 제안 ID 링크는 판매자가 비공개 제안 세부 정보에 액세스할 수 있도록 구매자에게 제공한 링크와 동일합니다.
- 수락 및 만료된 제안 탭에는 구매자가 수락하여 계약이 생성된 제안이 나열됩니다. 판매자가 설정한 제안 만료일이 경과한 제안도 나열됩니다. 이 탭은 판매자와 계약을 갱신할 때 이전 제안 ID 및 계약 ID(있는 경우)를 검색할 때 유용합니다. 제안을 수락하여 계약을 체결하고 계약이 활성 상태인 경우 계약을 선택하면 구독 세부 정보 페이지를 볼 수 있습니다.

> **Note**
>
> 미래 날짜의 비공개 제안은 조기 갱신으로 표시됩니다. 자세한 내용은 the section called “미래 날짜의 계약 관련 작업” 섹션을 참조하세요.

비공개 제안의 수정, 업그레이드 또는 갱신에 대한 자세한 내용은 비공개 제안 수정 또는 구독 해지 섹션을 참조하세요.

비공개 제안 페이지를 보는 데 필요한 권한

AWS Marketplace 콘솔에서 비공개 제안 페이지를 보려면 다음과 같은 권한이 있어야 합니다.

- AWS 관리형 정책을 사용하는 경우: `AWSMarketplaceRead-only`, `AWSMarketplaceManageSubscriptions` 또는 `AWSMarketplaceFullAccess`
- AWS 관리형 정책을 사용하지 않는 경우: IAM 작업 `aws-marketplace:ListPrivateListings`및 `aws-marketplace:ViewSubscriptions`

비공개 제안 페이지를 볼 수 없는 경우 관리자에게 문의하여 올바른 AWS Identity and Access Management(IAM) 권한을 설정합니다. AWS Marketplace에 필요한 IAM 권한에 대한 자세한 내용은 AWS Marketplace 구매자에 대한 AWS 관리형 정책 섹션을 참조하세요.

SaaS 비공개 제안 구독

서비스형 소프트웨어(SaaS) 비공개 제안의 경우 판매자와 협상할 수 있는 계약에 따라 사용 가능한 구성 옵션이 달라집니다.

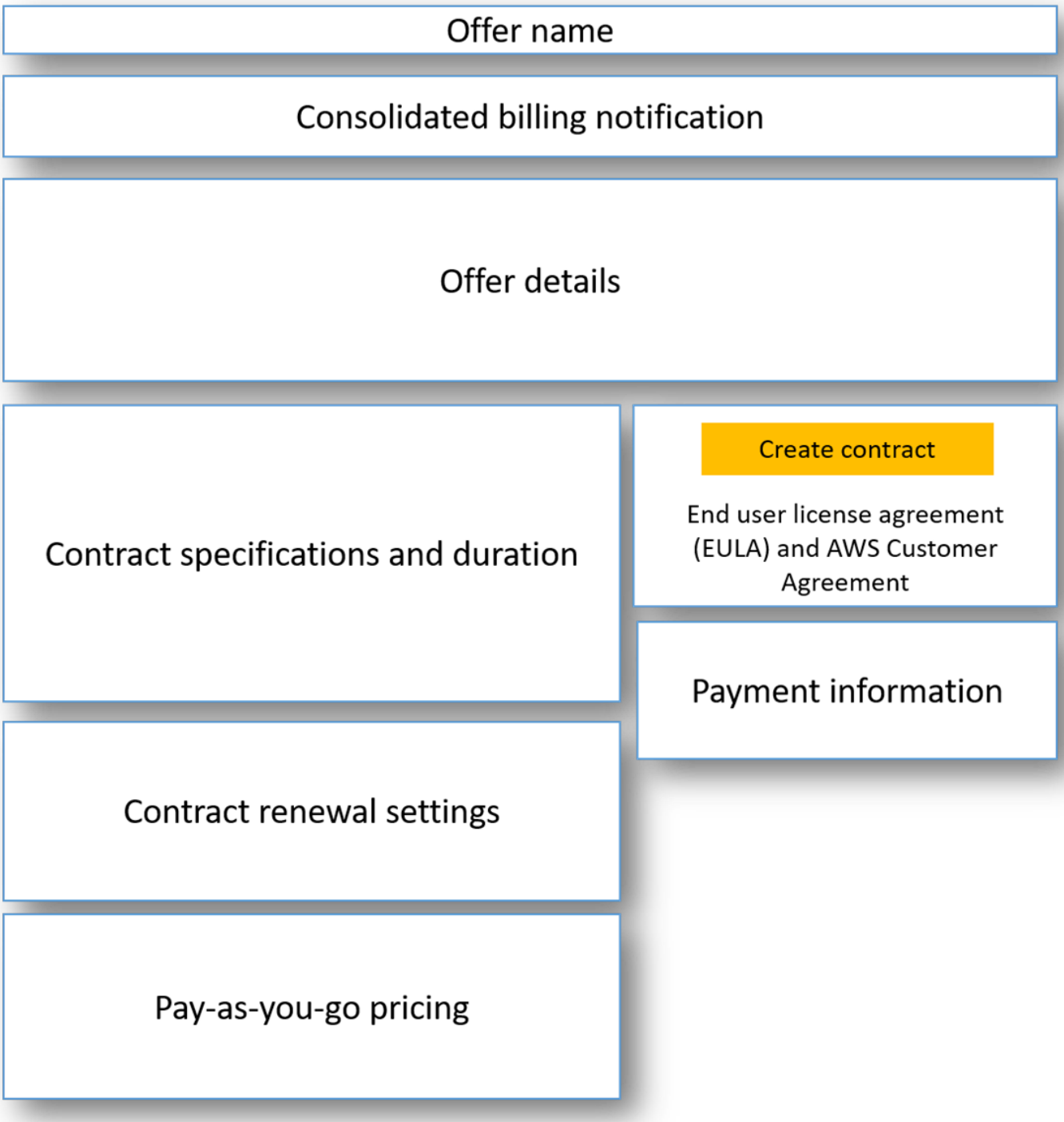
다음 다이어그램처럼 비공개 제안 페이지에는 다음과 같은 섹션이 있습니다.

- 제안 이름 - 판매자가 비공개 제안을 생성할 때 지정한 이름입니다.
- 통합 결제 정보 - 이 알림은 AWS 계정에 통합 결제를 사용할 때 표시됩니다.
- 계약 사양 및 기간 - 이 창에는 제안 기간과 제안을 정의하는 범위가 표시됩니다. 범위는 사용량 측정 방식과 협상 가격이 유효한 기간을 설명합니다(예: 12개월간 5GB/일 또는 시간당 사용자마다 $0.01). 비공개 제안이 계약인 경우, 계약 기간 동안 합의된 사용량에 대해 비용을 지불합니다. 비공개 제안이 구독인 경우, 측정된 사용량에 대해 합의된 요금으로 비용을 지불합니다.

> **Note**
>
> 미래 날짜의 비공개 제안은 조기 갱신으로 표시됩니다. 자세한 내용은 the section called “미래 날짜의 계약 관련 작업” 섹션을 참조하세요.

- 계약 갱신 설정 - 비공개 제안은 자동으로 갱신되도록 설정할 수 없습니다. SaaS 제품에 대한 비공개 제안의 경우, 이 창은 항상 이 제안에 대한 갱신이 없음을 나타냅니다.
- 사용량에 따른 요금 - 비공개 제안에 정의된 요금 이상으로 제품 사용 요금을 협상한 경우 추가 사용 비용에 대한 내역이 여기에 표시됩니다. 예를 들어 12개월간 5GB/일의 데이터 스토리지를 사용하기로 SaaS 계약에 합의했는데 10GB/일을 사용한 경우, 첫 5GB는 계약으로 커버됩니다. 추가 5GB/일은 종량 과금제로 청구됩니다. SaaS 구독을 이용하면 계약 기간 동안 얼마나 사용하든 합의된 요금만 냅니다.
- 최종 사용자 라이선스 계약(EULA) 및 계약 생성 버튼 - 판매자가 이 비공개 제안과 관련하여 업로드한 라이선스 계약을 볼 수 있습니다. 또한 여기에서 모든 비공개 제안 사양을 본 후 계약을 체결할 준비가 되면 계약을 수락할 수 있습니다.
- 결제 정보 - 이 창에서는 결제 기한, (결제 일정을 협상한 경우) 결제 기한의 날짜 및 시간을 설명합니다.

> **Important**
>
> 비공개 제안 페이지에 아무 섹션도 없으면 비공개 제안에서 협상이 이루어지지 않았기 때문입니다.



SaaS 비공개 제안을 구독하는 방법

1. 비공개 제안 확인 및 구독 섹션의 단계를 따릅니다.

2. 제안 세부 정보 창에서 올바른 비공개 제안을 선택했는지 확인합니다. 제품에 대해 제안이 여러 개 있을 수 있습니다.
3. 계약 사양 및 기간 창에서 계약 기간 및 계약 세부 정보가 협상된 내용인지 확인합니다. 그렇지 않은 경우 올바른 비공개 제안을 선택했는지 확인하거나 제안을 생성한 판매자에 문의하십시오.

> **Note**
>
> 미래 날짜의 비공개 제안은 조기 갱신으로 표시됩니다. 자세한 내용은 the section called "미래 날짜의 계약 관련 작업" 섹션을 참조하세요.

4. 종량 과금제를 협상한 경우, 협상한 조건을 설명하는 정보가 포함된 창이 있을 것입니다. 이 정보를 확인하거나, 이 정보를 보고자 하는데 없는 경우 해당 판매자에 문의하십시오.
5. 결제 정보 창에서 결제 정보를 확인합니다. 유연한 결제 일정을 협상한 경우, 결제 날짜 및 금액이 표시됩니다. 그렇지 않은 경우, 제안 수락 시 총 계약 금액이 청구됩니다.
6. EULA 및 계약 생성 창에서 EULA가 판매자와 협상한 것인지 확인합니다. 계약 이용 약관을 모두 검토한 후 Create contract(계약 생성)를 선택하여 제안을 수락합니다.

제안을 수락하면 제품을 성공적으로 구독했다는 내용의 확인 페이지가 열립니다. Set Up Your Account(계정 설정)를 선택하여 판매자의 페이지로 이동하고 판매자의 웹 사이트에서 계정 구성을 마칩니다.

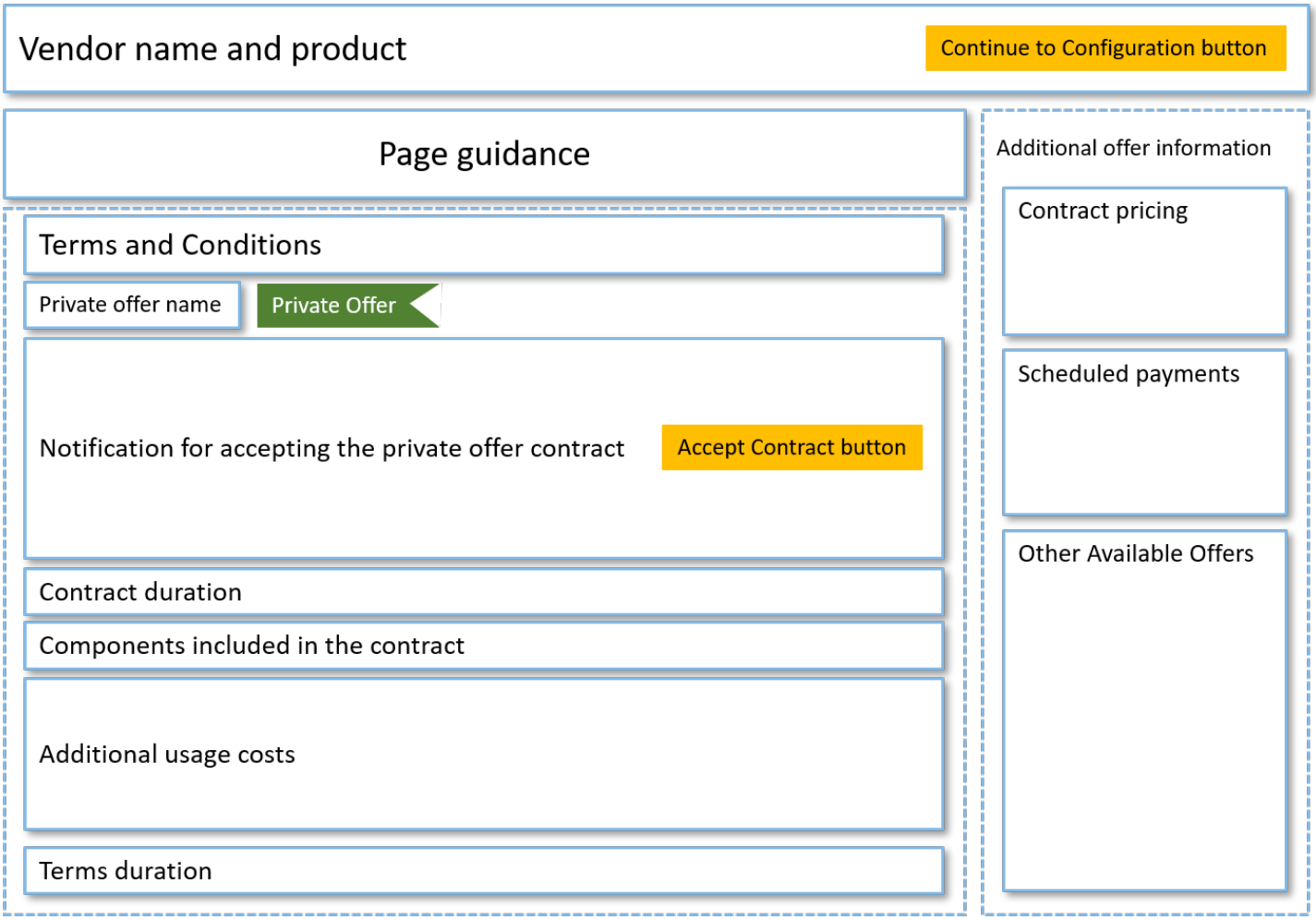
AMI 비공개 제안 구독

Amazon Machine Image(AMI) 비공개 제안에 사용할 수 있는 섹션과 구성 옵션은 제품 공급업체와 협상하는 계약에 따라 달라집니다. 다음 이미지는 AWS Marketplace 웹 사이트의 AMI 비공개 제안 페이지 레이아웃을 보여줍니다.

다음 다이어그램처럼 비공개 제안 페이지에는 다음과 같은 섹션이 있습니다.

- 공급업체 이름 및 제품 - 공급업에 이름과 비공개 제안 대상인 제품입니다. 오른쪽은 제품의 구성 버튼입니다.
- 페이지 지침 - 이 영역에는 이 페이지의 작업을 완료하고 비공개 제안을 수락하는 것과 관련된 지침이 있습니다.
- 이용 약관 - 이 섹션에는 다음 정보가 있습니다.
  - 왼쪽 위에는 비공개 제안의 이름과 해당 제안이 비공개 제안임을 나타내는 레이블이 있습니다.

  - 비공개 제안 이름 섹션 아래에는 계약 수락 알림이 있습니다. 계약 수락 버튼을 사용하여 비공개 제안을 수락할 수 있습니다.
  - 알림 섹션 아래에는 계약 기간, 계약에 포함된 구성 요소, 협상한 인스턴스 요금에 대한 섹션이 있으며, 여기에서도 EULA를 보거나 다운로드할 수 있습니다.
- 계약 기간 - 이 섹션에는 계약 일수와 계약 종료일이 표시됩니다.
- 추가 제안 정보 - 오른쪽에는 총 계약 요금, 예정된 다음 결제, 현재 약관, 기타 이용 가능한 비공개 및 공개 제안의 썸네일 이미지가 있습니다.



유연한 결제 일정이 적용되는 연간 AMI 비공개 제안 구독

AMI 비공개 제안을 구독하려면 AWS Marketplace 웹 사이트에서 비공개 제안을 수락해야 합니다. AWS Marketplace 콘솔 또는 Amazon Elastic Compute Cloud(Amazon EC2) 콘솔에서는 비공개 제안을 수락할 수 없습니다. 판매자가 유연한 결제 일정이 적용되는 비공개 제안을 생성하는 경우 비공개

제안에 표시된 금액이 결제 예정일에 청구됩니다. 유연한 결제 일정이 적용되는 AMI 비공개 제안을 수락하려면 다음 절차를 진행합니다.

유연한 결제 일정이 적용되는 AMI 비공개 제안을 수락하는 방법

1. 비공개 제안 확인 및 구독 섹션의 단계를 따릅니다.
2. 올바른 비공개 제안을 보고 있는지 확인합니다. 공급업체는 자사 제품에 대한 비공개 제안을 여러 개 생성할 수 있습니다. 모든 추가 비공개 제안은 사용 가능한 기타 제안 섹션에 표시됩니다.
3. 제안 만료 날짜와 요금 정보가 해당 비공개 제안에 대해 협상한 내용인지 확인합니다. 아닌 경우 올바른 비공개 제안을 보고 있는지 확인합니다.
4. EULA를 다운로드하고 EULA가 해당 비공개 제안에 대해 협상한 내용인지 확인합니다.
5. 계약 기간 섹션에서 비공개 제안의 조건이 협상한 내용과 일치하는지 확인합니다.
6. 비공개 제안의 세부 정보를 확인한 후에는 이용 약관 섹션에서 계약에 동의를 선택합니다.
7. 약관을 검토하고 동의할 경우 확인을 선택합니다.

> **Important**
>
> 시스템에서 계약 요청을 처리하는 동안 브라우저를 새로 고치지 마세요.

AMI를 구성할 준비가 되면 Continue to Configuration(구성 계속)을 선택합니다. 각 제품 사용에 대해 구독 프로세스를 완료해야 합니다.

유연한 결제 일정이 적용되지 않는 연간 AMI 비공개 제안 구독

AMI 비공개 제안을 구독하려면 AWS Marketplace 웹 사이트에서 비공개 제안을 수락해야 합니다. AWS Marketplace 콘솔 또는 Amazon EC2 콘솔에서는 비공개 제안을 수락할 수 없습니다. 판매자가 유연한 결제 일정이 적용되지 않는 비공개 제안을 생성하는 경우 계약에 동의하는 순간, 비공개 제안에 책정된 가격 및 옵션에 따라 계약을 구성할 수 있습니다. 유연한 결제 일정이 적용되지 않는 AMI 비공개 제안을 수락하려면 다음 절차를 진행합니다.

유연한 결제 일정이 적용되지 않는 AMI 비공개 제안을 수락하는 방법

1. 올바른 비공개 제안을 보고 있는지 확인합니다. 공급업체는 자사 제품에 대한 비공개 제안을 여러 개 생성할 수 있습니다. 추가 비공개 제안은 추가 비공개 제안 창에 표시됩니다. 수락하려는 제안이 이 제안 보기로 표시되는지 확인합니다.

> **Note**
>
> 많은 경우에 지급인 계정은 제품을 사용하는 계정이 아닙니다. 지급인 계정을 사용하여 제안을 수락하는 경우 원클릭 옵션을 선택하는 대신에 제품을 수동으로 시작하는 것이 좋습니다.

2. 제안 만료 날짜와 요금 정보가 해당 비공개 제안에 대해 협상한 내용인지 확인합니다. 아닌 경우 올바른 비공개 제안을 보고 있는지 확인합니다.
3. EULA를 다운로드하고 EULA가 해당 비공개 제안에 대해 협상한 내용인지 확인합니다.
4. 계약 조건 창에서 비공개 제안의 조건이 협상한 내용인지 확인합니다.
5. 제안 세부 내용이 비공개 제안에 대해 협상한 내용과 같은지 확인한 다음 조건 수락을 선택합니다. 아닌 경우 올바른 비공개 제안을 보고 있는지 확인합니다.
6. 이 소프트웨어 구독의 인스턴스 유형에서 사용 가능한 인스턴스 유형 목록 중에 선택합니다. 수량에서 라이선스 수량을 선택합니다.
7. 선택한 내용을 검토합니다. 이상 없으면 계약 생성을 선택하고 확인을 선택합니다.

AMI를 구성할 준비가 되면 Continue to Configuration(구성 계속)을 선택합니다. 각 제품 사용에 대해 구독 프로세스를 완료해야 합니다.

비공개 제안 수정 또는 구독 해지

스탠다드 구독에서 비공개 제안으로 업데이트하고, AWS Marketplace의 기존 비공개 제안을 수정할 수도 있습니다. 이 프로세스는 계약에 따라 다릅니다.

많은 구독의 경우 공개 가격에서 비공개 제안으로 바꿀 때 ISV 또는 채널 파트너와 제안을 협상합니다. 비공개 제안을 수락하면 기존의 관련 구독이 비공개 제안 가격 모델로 자동으로 이동합니다. 여기에는 어떤 추가 작업도 필요하지 않습니다. 다음 지침에 따라 시나리오를 확인하고 비공개 제안의 요금 수신을 시작하는 단계를 알아봅니다.

공개에서 비공개 제안 요금으로 변경

비공개 제안을 수락한 후 제안을 수락한 사용자에 대해 수행해야 하는 추가 작업은 없습니다. 비공개 제안에 정의된 요금 및 이용 약관으로 전환됩니다. 비공개 제안의 요금 및 이용 약관으로 전환하려면 해당 제품을 사용하는 연결된 각 사용자가 비공개 제안을 수락해야 합니다. 또한 해당 제품을 사용하기 시작하는 모든 사용자는 비공개 제안에 정의된 요금 및 이용 약관을 적용받으려면 비공개 제안을 수락해야 합니다.

SaaS 계약 변경 - 업그레이드 및 갱신

이 섹션은 서비스형 소프트웨어(SaaS) 계약 및 소비 제품과 체결하는 SaaS 계약에 적용됩니다. 이전 비공개 제안에서 체결한 계약이 유효한 상태에서 구매자가 동일한 제품에 대한 새 비공개 제안을 수락하려는 경우 판매자가 기존 계약을 업그레이드 또는 갱신하여 약관, 요금 또는 기간을 수정하거나 기존 계약이 종료되기 전에 계약을 갱신할 수 있습니다. 그러면 기존 계약을 먼저 취소할 필요 없이 새 비공개 제안을 수락할 수 있습니다.

> **Note**
>
> 미래 날짜의 비공개 제안은 조기 갱신으로 표시됩니다. 자세한 내용은 the section called “미래 날짜의 계약 관련 작업” 섹션을 참조하세요.

업그레이드 또는 갱신을 수락하려면 인보이스 발행 조건을 충족해야 합니다. 현재 인보이스 발행 조건을 충족하지 않은 경우 AWS고객 서비스에 티켓을 제출하여 결제 방법을 인보이스 발생으로 변경하세요.

결제 방법을 인보이스 발행으로 전환하지 않으려면 다음 조치 중 하나를 수행합니다.

- 제품 공급업체 및 AWS Marketplace 고객 지원 팀과 협력하여 현재 계약을 취소한 후 해당 제품에 대한 새 비공개 제안을 수락합니다.
- 다른 AWS 계정에서 제안을 수락합니다.

SaaS 구독에서 SaaS 계약으로 변경

SaaS 구독에서 SaaS 계약으로 변경하려면 먼저 SaaS 구독을 구독 해지해야 합니다. 그런 다음 SaaS 계약의 비공개 제안을 수락합니다. 기존 SaaS 구독을 보려면 AWS Marketplace 콘솔의 오른쪽 위 모서리에서 내 Marketplace 소프트웨어를 선택합니다.

AMI 계약을 새로운 계약으로 변경

이전 비공개 제안에서 Amazon Machine Image(AMI) 계약을 체결했고 동일한 제품에 대해 새로운 비공개 제안을 수락하려면 다음 중 하나를 수행해야 합니다.

- 현재 AMI 계약이 만료되기를 기다렸다가 새 AMI 계약을 수락합니다.
- 제품 공급업체 및 AWS Marketplace 고객 지원 팀과 협력하여 현재 계약을 종료합니다.
- 계약을 맺은 계정과 다른 AWS 계정을 사용하여 비공개 제안을 수락합니다.

AMI 시간별 구독에서 AMI 연간 구독으로 변경

AMI 시간별 구독에서 AMI 연간 구독으로 이동하더라도 구독은 바우처 시스템과 비슷하게 작동합니다. AMI의 매 사용 시간은 AMI 연간 구독에서 한 단위씩 차감 계산됩니다. 비공개 제안을 통해 연간 구독을 구매하면 해당 제품을 구독하는 연결된 모든 계정이 비공개 제안에서 협상된 요금으로 자동 전환됩니다. 비공개 제안이 수락된 후 구독을 시작하는 연결된 계정은 구독 시 비공개 제안을 구독해야 합니다.

> **Note**
>
> 기존 제안에 대한 연간 라이선스는 새로운 제안의 조건을 수락하는 즉시 비활성화됩니다. ISV와 기존 라이선스에 대한 보상과 새 제안을 추진하는 방법을 논의할 수 있습니다.

AMI 연간 구독에서 AMI 시간별 구독으로 변경

연간 구독이 만료된 후 해당 제품을 구독하는 연결된 모든 계정은 AMI 시간별 요금으로 자동 전환됩니다. 연간 구독을 맺은 상태에서는 연결된 계정이 해당 구독을 취소하지 않고는 해당 제품에 대한 시간별 구독으로 전환할 수 없습니다.

미래 날짜의 계약 및 비공개 제안 관련 작업

AWS Marketplace에서 미래 날짜의 계약(FDA)이 적용되면 미래 날짜부터 제품 사용이 시작되는 제품을 구독할 수 있습니다. 제품 구매 시기와 제품 사용 시기를 별도로 관리할 수 있습니다.

FDA는 구매자가 AWS Marketplace에서의 거래에 대해 독립적으로 다음과 같은 조치를 수행할 수 있도록 지원합니다.

- 제안을 수락하여 제품을 구매하거나 거래를 예약합니다.
- 제품 사용을 시작합니다(라이선스/권한 활성화).
- 구매 비용을 지불합니다(인보이스 생성).

FDA는 비공개 제안, 서비스형 소프트웨어(SaaS) 제품 제작, 유연한 결제 일정의 포함 여부에 관계없이 SaaS 계약 및 소비량 가격 책정 계약에 대해 지원됩니다.

미래 날짜의 계약을 사용할 때는 다음 날짜를 염두에 두십시오.

계약 체결 날짜

제안을 수락한 날짜와 계약이 생성된 날짜입니다. 이 날짜는 계약 ID가 생성되는 날짜입니다.

계약 시작 날짜

제품 사용이 시작되는 날짜입니다. 미래 날짜 또는 미래 시작 날짜입니다. 이 날짜는 라이선스/자격이 활성화된 날짜입니다.

계약 종료 날짜

계약의 종료일입니다. 계약 및 라이선스/자격은 이 날짜에 만료됩니다.

FDA 사용에 관한 자세한 내용은 다음 주제를 참조하십시오.

주제

- 미래 날짜의 계약서 작성
- 미래 날짜의 계약과 함께 유연한 결제 스케줄러 사용
- 미래 날짜의 계약 수정
- 미래 날짜의 계약에 대한 알림 받기

미래 날짜의 계약서 작성

유연한 결제 일정의 포함 여부에 관계없이 SaaS 계약 및 소비량 가격 책정 계약의 경우 판매자는 비공개 제안 생성의 일환으로 계약 시작일을 설정합니다. 구매자는 판매자와 협력하여 시작일이 요구 사항을 충족하는지 확인해야 합니다.

미래 날짜의 계약을 생성하려면 다음 절차를 사용하십시오. AWS Marketplace 콘솔의 구독 관리 페이지에서 미래 날짜의 계약을 볼 수 있습니다.

미래 날짜의 계약을 생성하려면

1. 비공개 제안 확인 및 구독 섹션의 단계를 따릅니다.
2. 제안 세부 정보 창에서 올바른 비공개 제안을 선택했고 계약 시작일이 정확한지 확인하십시오. 미래 날짜의 제안은 제안 드롭다운 메뉴에서 조기 갱신으로 표시됩니다.

> **Note**
>
> SaaS 제품의 경우 계약 시작일에 ISV에서 계정 설정을 완료해야 합니다. 계약 시작일 이전에는 이 단계를 완료할 수 없습니다. 자세한 내용은 the section called “SaaS 비공개 제안 구독” 단원을 참조하십시오.

미래 날짜의 계약과 함께 유연한 결제 스케줄러 사용

유연한 결제 스케줄러를 미래 날짜의 계약과 함께 사용할 수 있습니다. 계약 서명일과 계약 종료일 사이의 원하는 시점에 구매에 대한 결제를 설정할 수 있습니다. 이 접근 방식에는 계약 시작일 이전 및 이후의 결제가 포함됩니다.

비공개 제안을 생성하는 레코드 판매자가 결제 날짜와 금액을 선택합니다. 자세한 내용은 유연한 결제 스케줄러를 참조하십시오.

미래 날짜의 계약 수정

계약 시작일 이전과 이후에 FDA에서 특정 규격의 구매 단위를 늘릴 수 있습니다. 이 옵션은 약정서에 유연한 지급 일정이 없는 경우 사용할 수 있습니다. 자세한 내용은 유연한 결제 스케줄러를 참조하십시오.

수정이 완료되면 계약 시작일에 비례 할당으로 계산된 금액이 청구됩니다. 시작일이 과거인 경우 즉시 요금이 청구됩니다.

미래 날짜의 계약에 대한 알림 받기

미래 날짜의 계약에 대해 취해진 다음 조치에 대해 지정된 루트 계정으로 전송되는 이메일 알림을 받게 됩니다.

- 제안 수락/계약 생성(계약 서명일)
- 라이선스 또는 권한 활성화 시(계약 시작일)
- 30일, 60일 또는 90일 후에 만료되는 계약에 대한 사전 알림
- 계약 만료(계약 종료일)
- 계약 수정 또는 교체 시

조직 내에서 구독 공유

AWS Marketplace에서 제품을 구독하면 해당 제품을 사용할 수 있는 라이선스를 부여하는 계약이 생성됩니다. AWS 계정이 조직의 구성원인 경우 Amazon Machine Image(AMI), 컨테이너, 기계 학습 및 데이터 제품의 라이선스를 해당 조직의 다른 계정과 공유할 수 있습니다. AWS Marketplace에서 라이선스 지원을 설정한 다음, AWS License Manager 내부에서 라이선스를 공유해야 합니다.

> **Note**
>
> AWS Organizations에 대한 자세한 내용은 사용 설명서AWS Organizations를 참조하세요. AWS License Manager에서 조직과 라이선스를 공유하는 방법에 대한 자세한 내용은 AWS License Manager 사용 설명서의 권한 부여된 라이선스를 참조하세요.

다음 비디오에서는 라이선스 공유 경험을 안내합니다.

AWS Marketplace 라이선스 권한 배포(3:56)

다음 주제에서는 모든 계정에서 라이선스를 보고, 공유하고, 추적하는 프로세스를 간략하게 설명합니다.

주제

- 라이선스를 공유하기 위한 사전 조건
- 라이선스 보기
- 라이선스 공유
- 라이선스 사용 추적

라이선스를 공유하기 위한 사전 조건

AWS Marketplace에서 라이선스를 공유하려면 먼저 조직의 라이선스 공유를 설정해야 합니다. 조직의 라이선스 공유를 설정하려면 다음 작업을 완료합니다.

- 라이선스를 구매하거나 라이선스를 공유할 때 관련 라이선스 권한 부여를 생성할 수 있도록, 구매자 대신 라이선스를 관리할 수 있는 AWS Marketplace 권한을 부여합니다. 자세한 내용은 역할을 사용하여 AWS Marketplace에 대한 권한 공유 섹션을 참조하세요.
- 최초 사용에 대해 AWS License Manager를 설정합니다. 자세한 내용은 AWS License Manager 사용 설명서의 AWS License Manager 시작하기를 참조하세요.

라이선스 보기

AWS Marketplace는 구매자가 구매한 AMI, 컨테이너, 기계 학습, 서비스형 소프트웨어(SaaS) 및 데이터 제품에 대한 라이선스를 자동으로 생성합니다. 구매자는 이러한 라이선스를 조직 내 다른 계정과 공유할 수 있습니다.

> **Note**
>
> SaaS 제품의 라이선스가 생성되었지만, 현재는 SaaS 라이선스를 공유할 수 없습니다.

AWS License Manager를 사용하여 라이선스를 관리하고 공유하세요. 하지만 AWS Marketplace를 사용하여 AWS Marketplace 내에서 구매한 제품의 라이선스를 보는 것은 가능합니다.

AWS Marketplace에서 구독한 제품의 라이선스를 보는 방법

1. AWS Marketplace에 로그인하고 구독 관리를 선택합니다.
2. 모든 라이선스를 볼 수도 있고 특정 구독의 라이선스만 볼 수도 있습니다.
   - 모든 라이선스를 보는 방법
     - 작업 메뉴에서 라이선스 보기를 선택하여 License Manager 콘솔의 모든 AWS Marketplace 관리형 라이선스를 봅니다.
   - 단일 구독의 라이선스를 보는 방법
     a. 보려는 제품의 카드를 선택하여 제품 세부 정보 페이지로 이동합니다.
     b. 작업 메뉴에서 라이선스 보기를 선택하여 License Manager 콘솔에서 해당 제품의 라이선스를 봅니다.

> **Note**
>
> 조직의 모든 계정에서 집계한, 권한 부여된 라이선스를 볼 수도 있습니다. 자세한 내용을 알아보려면 AWS License Manager 사용 설명서의 권한 부여된 라이선스를 참조하세요.

라이선스 공유

AMI, 컨테이너, 기계 학습 및 데이터 제품의 라이선스만 공유할 수 있습니다.

AWS Marketplace의 구독은 다음과 같이 제품 세부 정보에 액세스 수준이 표시됩니다.

- 계약 수준의 제품은 구매자가 사용하고 조직 내 다른 계정과 공유할 수 있는 라이선스가 있습니다.
- 권한 수준의 제품은 구매자의 계정과 공유되는 라이선스입니다. 이러한 제품을 사용할 수는 있지만 공유할 수는 없습니다.

AWS Marketplace는 AWS License Manager를 사용하여 AWS Organizations, AWS 계정 또는 조직 단위와 직접 라이선스 사용을 공유하는 권한 부여를 지원합니다. 이제 권한 부여 활성화 프로세스에는 AWS Marketplace에서 조달한 동일한 제품에 대해 활성화된 권한 부여를 대체할 수 있는 추가 옵션이 있습니다. 자세한 내용을 알아보려면 AWS License Manager 사용 설명서의 부여된 라이선스를 참조하세요.

> **Note**
>
> 특정 AWS 리전으로 제한되는 제품의 경우 라이선스를 공유하는 계정은 해당 계정이 허용된 리전 내에 있는 경우에만 라이선스를 활성화할 수 있습니다.

라이선스 사용 추적

AWS License Manager에서 각 라이선스의 사용 대시보드 탭을 선택하여 AMI 제품의 사용량 기반 라이선스 지표를 추적할 수 있습니다.

License Manager를 사용하여 라이선스 사용을 추적하는 방법에 대한 자세한 내용은 AWS License Manager 사용 설명서의 권한 부여된 라이선스를 참조하세요.

AWS Marketplace 이벤트에 대한 구매자 알림

AWS Marketplace는 이메일, Amazon EventBridge 이벤트 및 Amazon Simple Notification Service(SNS) 주제를 통해 적시에 알림을 제공합니다.

주제

AWS Marketplace 이벤트에 대한 이메일 알림

AWS Marketplace의 구매자는 다음 중 하나가 발생할 때 이메일 알림을 받습니다.

- 구매자가 제안을 수락합니다.
- 판매자가 이전에 구매자가 수락한 비공개 제안과 관련된 새 비공개 제안을 게시하거나 이전에 수락한 제안에 대한 업데이트를 게시합니다.

> **Note**
>
> 알림은 구매자 AWS 계정 ID와 연결된 이메일 주소로 전송됩니다.

AWS Marketplace 이벤트에 대한 Amazon EventBridge 알림

AWS Marketplace는 Amazon EventBridge(이전에는 Amazon CloudWatch Events)와 통합됩니다. EventBridge는 애플리케이션을 다양한 소스의 데이터와 연결하는 데 사용할 수 있는 이벤트 버스 서비스입니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.

구매자는 판매자가 제안을 생성하여 구매할 수 있게 할 때마다 AWS Marketplace에서 이벤트를 받습니다. 이벤트에는 ID, 만료 날짜, 제품 세부 정보, 판매자 이름 등의 세부 정보가 포함되어 있습니다.

주제

AWS Marketplace Discovery API Amazon EventBridge 이벤트

이 주제는 다음 표에 나열된 각 이벤트에 대한 자세한 정보를 제공합니다.

판매자 조치	구매자가 받은 이벤트	관련 주제
제안을 생성하고 구매할 수 있게 만들기	`Listing Available`	the section called “새 목록 이벤트”

새 목록 이벤트

판매자가 제안을 생성하고 구매할 수 있게 만들면 구매자는 `Listing Available`이라는 상세 정보 유형의 이벤트를 받게 됩니다.

> **Note**
>
> EventBridge 규칙 생성에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 규칙을 참조하세요.

다음은 `Listing Available` 이벤트의 데이터 본문 예시입니다.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "Listing Available",
    "source": "aws.discovery-marketplace",
    "account": "123456789012",
    "time": "2023-08-26T00:00:00Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "requestId": "3d4c9f9b-b809-4f5e-9fac-a9ae98b05cbb",
        "catalog": "AWSMarketplace",
        "offer": {
            "id": "offer-1234567890123",
            "expirationDate": "2025-08-26T00:00:00Z"
        },
        "product": {
            "id": "bbbbaaaa-abcd-1111-abcd-666666666666",
```

```
            "title": "Product Title"
        },
        "sellerOfRecord": {
            "name": "Seller Name"
        }
    }
}
```

조달 시스템과 AWS Marketplace 통합

AWS Marketplace와 Coupa 또는 SAP Ariba 조달 소프트웨어의 통합을 구성할 수 있습니다. 구성을 완료한 후 조직의 사용자는 조달 소프트웨어를 사용하여 AWS Marketplace 제품에 대한 구독을 검색하고 요청할 수 있습니다. 구독 요청이 승인되면 트랜잭션이 완료되고, 소프트웨어 구독이 가능함을 사용자에게 알립니다. 사용자가 AWS Marketplace에 로그인하면 해당 소프트웨어 제품이 구입한 구독으로 표기되어 사용할 수 있습니다. 조달 시스템과 통합하면 AWS Marketplace 인보이스를 구매 주문 시스템과 통합할 수도 있습니다.

조달 통합의 작동 방식

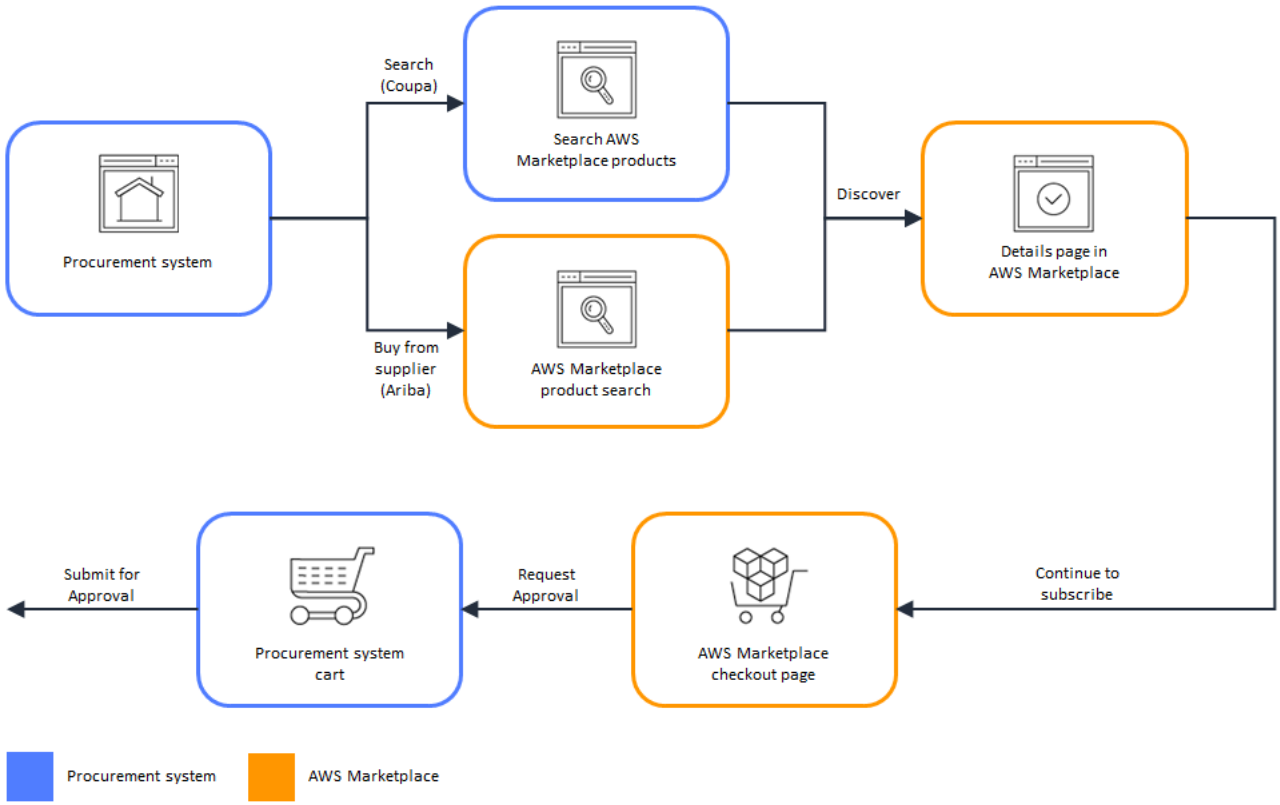
상업용 확장형 마크업 언어(cXML) 프로토콜을 따르는 AWS Marketplace와 통합하도록 조달 소프트웨어를 구성할 수 있습니다. 이 통합을 통해 타사 카탈로그에 대한 액세스 포인트, 즉 펀치아웃이 생성됩니다.

통합은 조달 시스템에 따라 조금씩 다릅니다.

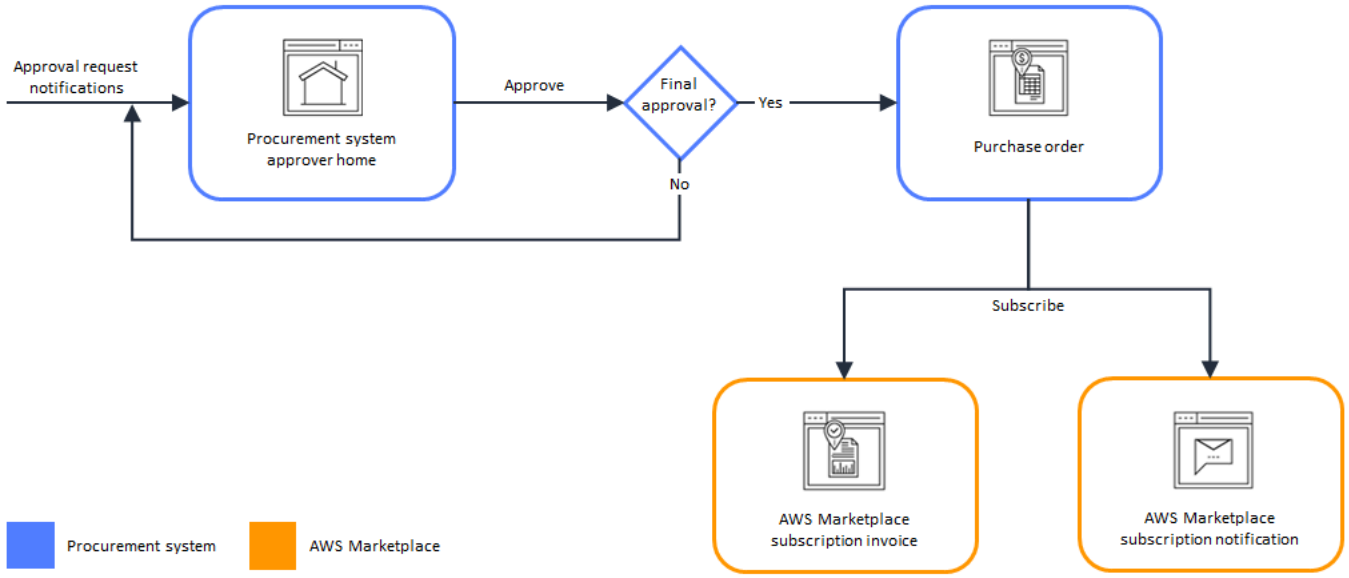
- Coupa - Coupa Open Buy 기능을 사용하면 Coupa 내에서 AWS Marketplace를 검색할 수 있습니다. Coupa는 검색 결과를 표시하고, 사용자가 제품을 선택하면 AWS Marketplace로 리디렉션되어 제품 세부 정보를 볼 수 있게 됩니다. 또는 Coupa의 조달 소프트웨어 사용자는 홈 페이지의 온라인 상점 섹션에서 AWS Marketplace 카탈로그에 액세스할 수 있습니다. 사용자는 AWS Marketplace에서 직접 제품 검색을 시작하도록 선택할 수도 있습니다.
- SAP Ariba - Ariba는 소프트웨어를 검색하고 제품 세부 정보를 볼 수 있는 AWS Marketplace로 사용자를 리디렉션합니다. 관리자가 펀치아웃 통합을 구성하면 Ariba의 조달 소프트웨어 사용자는 카탈로그 탭을 선택한 후 AWS Marketplace 카탈로그를 선택하여 AWS Marketplace 소프트웨어를 찾을 수 있습니다. 그러면 사용자가 원하는 제품을 찾을 수 있는 AWS Marketplace 페이지로 리디렉션됩니다.

  Ariba 사용자는 AWS Marketplace가 아닌 Ariba 내에서 구매를 시작해야 합니다.

사용자는 AWS Marketplace에서 검색 중인 구독을 구매하려면 AWS Marketplace 내에서 구독 요청을 생성해야 합니다. 사용자는 제품의 구독 페이지에 구매를 완료하는 대신 승인을 요청해야 합니다. 이 요청이 조달 시스템의 장바구니로 다시 전송되어 승인 과정이 완료됩니다. 다음 다이어그램은 조달 시스템 구독 요청 프로세스를 보여줍니다.



조달 시스템이 AWS Marketplace로부터 요청을 받으면 조달 시스템이 승인 프로세스를 완료하는 워크플로우를 시작합니다. 요청이 승인되면 조달 시스템의 구매 주문 시스템이 자동으로 AWS Marketplace의 거래를 완료하고, 사용자에게 구독을 배포할 준비가 완료되었음을 알립니다. 요청자는 구매를 완료하기 위해 AWS Marketplace로 돌아올 필요가 없습니다. 하지만 구매한 제품의 사용 지침을 보기 위해 AWS Marketplace를 다시 방문해야 할 수도 있습니다. AWS Marketplace는 AWS Marketplace에 액세스하는 데 사용된 AWS 계정으로 이메일 메시지를 보냅니다. 이메일 메시지는 구독이 성공했으며 AWS Marketplace를 통해 소프트웨어를 사용할 수 있다고 수신자에게 알리는 내용입니다. 다음 다이어그램은 조달 시스템 구독 요청 승인 프로세스를 보여줍니다.



조달 시스템과 통합할 때 다음과 같은 추가 참고 사항이 있습니다.

- 무료 평가판은 관련 요금이 부과되지 않기 때문에 조달 시스템에서 인보이스를 생성하지 않습니다.
- 사용한 만큼만 지불 요금 외에 일회성 요금이 부과되는 계약은 두 번의 승인이 필요할 수 있습니다. 하나는 계약(또는 연간) 요금에 대한 승인이고, 다른 하나는 시간당 또는 단가(사용한 만큼만 지불)에 대한 승인입니다.
- 조달 시스템 통합(PSI)을 사용하는 고객은 무료 제품 및 BYOL 제품에 대한 사전 승인을 활성화할 수 있습니다. 무료와 BYOL에 대해 각각 하나씩 총 두 가지 설정이 있습니다. 설정이 활성화되면 주문이 AWS Marketplace에서 사전 승인되므로, 고객은 승인을 받기 위해 조달 시스템에 주문을 제출할 필요가 없습니다. 설정이 비활성화되면 고객은 승인 요청 버튼을 통해 조달 시스템에 승인 요청을 제출해야 합니다. 무료 및 BYOL 제품에 대한 사전 승인 설정을 비활성화하면 고객의 조달 시스템에서 0.00 USD 주문이 생성됩니다. 조달 시스템 통합에 대한 자세한 내용은 https://aws.amazon.com/marketplace/features/procurementsystem 섹션을 참조하세요.

조달 시스템 통합 설정

AWS Marketplace와 조달 시스템의 통합을 구성하려면 AWS Marketplace에서 프로세스를 시작하고 조달 시스템에서 프로세스를 합니다. AWS Marketplace에서 생성된 정보를 사용하여 조달 시스템 펀치아웃을 구성합니다. 구성을 완료하려면 사용하는 계정이 다음 요구사항을 충족해야 합니다.

- AWS Marketplace 구성을 완료하는 데 사용된 AWS 계정이 관리 계정이어야 하며 `AWSMarketplaceProcurementSystemAdminFullAccess` 관리형 정책에 AWS Identity and Access Management(IAM) 권한이 정의되어 있어야 합니다.

- 구성을 완료하는 데 사용된 조달 시스템 계정이 조달 시스템에서 계약, 공급업체 및 펀치아웃을 설정할 수 있는 관리 권한이 있어야 합니다.

IAM 권한 구성

다음 IAM 권한은 AWS관리형 정책: AWSMarketplaceProcurementSystemAdminFullAccess 관리형 정책에 있으며 AWS Marketplace와 조달 시스템의 통합을 구성하는 데 필요합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

수동으로 권한을 구성하는 대신 IAM 관리 권한을 사용하는 것이 좋습니다. 이 방법을 사용하면 인적 오류가 덜 발생하고, 권한이 변경되면 관리 정책이 업데이트됩니다. AWS Marketplace에서 IAM을 구성하고 사용하는 방법에 대한 자세한 내용은 AWS Marketplace 보안 섹션을 참조하세요.

Coupa와 통합되도록 AWS Marketplace 구성

IAM 권한을 설정한 후에는 AWS Marketplace와 Coupa의 통합을 구성할 수 있습니다. 조달 관리로 이동합니다. 조달 시스템 관리 창에서 펀치아웃의 이름과 설명을 입력합니다. 준비가 완료될 때까지 제품 구독을 생성하지 않고 사용자가 통합을 테스트할 수 있도록, 통합을 테스트 모드로 전환할 수도 있습니다. 통합의 AWS Marketplace 부분을 구성하려면 다음 절차를 완료하십시오.

Coupa와 통합할 AWS Marketplace를 구성하려면

1. AWS Marketplace Manage Procurement Systems(조달 시스템 관리)의 Procurement systems(조달 시스템)에서 Set up Coupa integration(Coupa 통합 설정)을 선택하십시오.
2. Manage Coupa integration(Coupa 통합 관리) 페이지의 Account information(계정 정보) 아래에 통합의 이름과 설명을 입력하십시오.

   > **Note**
   >
   > AWS Billing 콘솔의 인보이스가 서비스형 소프트웨어(SaaS) 계약 제품을 구독하는 데 사용된 상업용 확장형 마크업 언어(cXML) 구매 주문을 참조하게 해야 하는 경우가 있습니다. 이 경우 AWS Marketplace 설정에서 서비스 연결 역할을 사용하여 결제 통합을 활성화하면 됩니다.

3. 리디렉션 활성화 및 테스트 모드의 구성 설정을 켜거나 끄고 저장을 선택하여 AWS Marketplace 시스템에서 통합을 완료할 수 있습니다.

AWS Marketplace에서 통합을 완료한 후에는 Coupa에서 통합을 설정해야 합니다. 이 페이지에서 생성된 정보를 사용하여 Coupa 시스템에 펀치아웃을 구성합니다.

AWS Marketplace 구성은 기본적으로 테스트 모드가 활성화되도록 설정됩니다. 테스트 모드에서는 구독 요청이 Coupa 백엔드로 이동하므로 전체 흐름을 볼 수 있지만, 최종 인보이스는 생성되지 않습니다. 그러면 구성을 완료하고 계획대로 펀치아웃을 활성화할 수 있습니다.

> **Note**
>
> 필요한 대로 테스트 모드를 켜거나 끌 수 있습니다.
> 통합을 완료한 후에는 잊지 말고 테스트 모드를 꺼야 합니다. 그렇지 않으면 시스템의 사용자가 요청을 생성하는 것처럼 보이지만 어떤 소프트웨어도 구매되지 않습니다.

Coupa 구성

Coupa 시스템에서 AWS Marketplace와의 통합을 구성하려면 AWS Marketplace의 Coupa 통합 관리 페이지에서 구매 정보 창에 있는 정보를 복사합니다. 이 정보를 사용하여 Coupa 조달 시스템 구성 방법을 안내하는 다음 링크의 단계를 완료합니다.

- Coupa 펀치아웃 설정

- cXML 구매 주문을 위한 공급자 구성

> **Note**
>
> AWS Marketplace에서 사용하는 UNSPSC 코드에 대한 자세한 내용은 AWS Marketplace에서 사용하는 UNSPSC 코드 섹션을 참조하세요.

SAP Ariba와 통합되도록 AWS Marketplace 구성

Ariba와 통합되도록 AWS Marketplace를 구성하려면 AWS Marketplace 운영 팀과 협력하여 레벨 1 펀치아웃을 생성해야 합니다. SAP Ariba 펀치아웃에 대한 자세한 내용은 SAP 커뮤니티 웹 사이트의 SAP Ariba 펀치아웃 소개를 참조하세요.

설정을 구성하기 위한 준비로 다음 정보를 수집합니다.

- 귀하의 AWS 계정 ID. AWS 계정이 AWS 조직에 속한 경우 관리 계정 ID도 필요합니다.
- SAP Ariba 시스템의 Ariba 네트워크 ID(ANID)도 필요합니다.

> **Note**
>
> Ariba의 ANID에 대한 내용과 Ariba에 대한 기타 질문에 대한 답변은 SAP Ariba 웹 사이트의 공급업체를 위한 Ariba 네트워크: FAQ 페이지를 참조하세요.

Ariba와 통합되도록 AWS Marketplace를 구성하는 방법

1. AWS Marketplace 조달 시스템 관리의 조달 시스템에서 Ariba 통합 설정을 선택합니다.
2. SAP Ariba 통합 관리 페이지의 계정 정보에 통합의 이름 및 설명과 Ariba 시스템의 SAP Ariba 네트워크 ID(ANID)를 입력합니다.

   > **Note**
   >
   > AWS Billing 콘솔의 인보이스가 SaaS 계약 제품을 구독하는 데 사용된 cXML 구매 주문을 참조하게 해야 하는 경우가 있습니다. 이 경우 AWS Marketplace 설정에서 서비스 연결 역할을 사용하여 결제 통합을 활성화하면 됩니다.

3. 테스트 모드를 활성화한 다음, 저장을 선택하여 AWS Marketplace 통합 설정을 저장합니다.

4. SAP Ariba 통합 생성 프로세스를 시작하려면 AWS에 문의하세요. 위 정보를 포함해야 합니다. AWS Marketplace에서 Ariba 통합을 설정하고 테스트하는 방법에 대한 지침을 보내드립니다.

> **Note**
>
> AWS Marketplace와 공급업체 관계를 생성하려면 SAP Ariba 시스템에 대한 관리자 액세스 권한이 필요합니다.

AWS Marketplace 팀의 지침 및 구성 설정에 따라 SAP Ariba 테스트 환경에서 통합을 생성하고, AWS Marketplace를 테스트 모드로 실행합니다. 테스트 환경에서는 구독 요청이 Ariba 백엔드로 이동하므로 AWS Marketplace에서 구독을 생성하지 않아도 승인을 포함한 전체 흐름을 볼 수 있으며, 인보이스가 생성되지 않습니다. 이 접근 방식을 사용하면 구성을 테스트한 후 프로덕션 환경에서 펀치아웃을 활성화할 수 있습니다. 테스트가 완료되고 프로덕션으로 전환할 준비가 되면 AWS에 문의하여 프로덕션 환경에서 계정을 설정합니다.

> **Note**
>
> 통합 테스트를 마친 후에는 잊지 말고 프로덕션으로 전환해야 합니다. 그렇지 않으면 시스템의 사용자는 자신이 요청을 생성하고 있다고 생각하지만 어떤 소프트웨어도 구매되지 않습니다.

테스트를 마치고 AWS Marketplace 팀과 협력하여 테스트 모드를 끄면 통합이 완료됩니다.

SAP Ariba 구성에 대한 자세한 내용은 SAP Ariba의 다음 주제를 참조하세요.

- SAP Ariba 웹 사이트의 SAP Ariba 펀치아웃
- SAP 커뮤니티 웹 사이트의 SAP Ariba 펀치아웃 소개

> **Note**
>
> AWS Marketplace에서 사용하는 UNSPSC 코드에 대한 자세한 내용은 AWS Marketplace에서 사용하는 UNSPSC 코드 섹션을 참조하세요.

AWS Marketplace에서 사용하는 UNSPSC 코드

AWS Marketplace는 조달 카트로 다시 반환되는 소프트웨어 목록에 UN 표준 제품 및 서비스 코드(UNSPSC) 43232701을 사용합니다.

조달 시스템 통합 비활성화

Coupa 또는 SAP Ariba와의 통합을 비활성화하려면 조달 시스템 내에서 펀치아웃 통합을 제거해야 합니다. 그러려면 Coupa 또는 Ariba 내에서 AWS Marketplace의 자동 리디렉션 기능을 비활성화합니다. 그러면 통합이 비활성화되지만 설정은 유지되므로 쉽게 다시 활성화할 수 있습니다.

AWS Marketplace 쪽의 통합 설정을 완전히 제거해야 하는 경우 AWS에 문의해야 합니다.

무료 평가판

AWS Marketplace에 등록된 일부 제품은 무료 평가판을 제공하고 있습니다. 소프트웨어를 구매하기 전에 무료 평가판을 통해 미리 체험해볼 수 있습니다. 무료 평가판은 무료 사용량이 제한되거나 무료 사용 시간이 제한됩니다. 무료 평가판을 시작한 후에는 무료 기간을 일시 중지할 수 없습니다.

소프트웨어 및 인프라 요금

판매자가 제공하는 무료 평가판은 AWS Marketplace에 게시된 제품의 소프트웨어 요금에만 적용됩니다. 소프트웨어 요금에 무료 평가판이 포함되어 있는지 여부에 관계없이 AWS Marketplace의 제품을 사용하는 동안 발생하는 모든 인프라 비용은 구매자가 부담합니다. 인프라 비용은 AWS에서 책정하며 해당 가격 페이지에서 확인할 수 있습니다. 예를 들어 무료 평가판이 제공되는 Amazon Machine Image(AMI) 제품을 구독하는 경우 무료 평가판 기간에는 AMI 사용 요금이 부과되지 않습니다. 하지만 AMI 제품을 실행하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대한 요금이 부과될 수 있습니다.

> **Note**
>
> 일부 제품은 실행하려면 추가 AWS 인프라가 필요할 수 있습니다. 예를 들어 로드 밸런서, 스토리지, 데이터베이스 또는 기타 AWS 서비스를 AWS 계정에 배포하는 배포 지침이나 템플릿을 판매자가 제공할 수도 있습니다. 판매자가 제품에 요구하는 AWS 서비스를 확인하려면 AWS Marketplace에 게시된 제품의 세부 정보 페이지를 검토하세요. 그런 다음, 해당 AWS 서비스의 요금 페이지를 검토하세요.

AMI 기반 제품의 무료 평가판

시간당 요금 또는 시간당 요금과 연간 요금이 함께 적용되는 AWS Marketplace의 일부 AMI 제품은 무료 평가판을 제공합니다. 무료 평가판을 구독하면 시간당 소프트웨어 요금 없이 판매자가 설정한 기간 동안 AMI 제품의 Amazon EC2 인스턴스 하나를 실행할 수 있습니다. 인프라 비용은 구매자가 부담합니다. Amazon EC2 인스턴스를 추가로 시작하면 인스턴스마다 시간당 소프트웨어 요금이 발생합니다. 무료 평가판 기간이 만료되면 자동으로 유료 구독으로 전환됩니다.

무료 평가판 기간이 만료되기 전에 Amazon EC2 인스턴스를 종료하지 않으면 무료 평가판 기간이 만료될 때 시간당 소프트웨어 요금이 발생합니다. 무료 평가판 구독을 취소해도 Amazon EC2 인스턴스가 자동으로 종료되지 않으며, 계속 사용할 경우 소프트웨어 요금이 부과됩니다. 인프라 요금에 대한 자세한 내용은 Amazon EC2 요금을 참조하세요.

컨테이너 기반 제품의 무료 평가판

시간당 요금 또는 시간당 요금과 장기 요금이 함께 적용되는 AWS Marketplace의 일부 컨테이너 제품은 무료 평가판을 제공합니다. 무료 평가판을 구독하면 시간당 소프트웨어 요금 없이 여러 Amazon Elastic Container Service(Amazon ECS) 작업 또는 Amazon Elastic Kubernetes Service(Amazon EKS) 포드를 일정 기간 동안 실행할 수 있습니다. 포함된 작업 또는 포드 수와 무료 평가판 기간은 판매자가 설정합니다. 인프라 비용은 구매자가 부담합니다. 무료 평가판에 포함된 수를 초과하여 추가 작업 또는 포드를 시작하면 작업 또는 포드마다 시간당 소프트웨어 요금이 부과됩니다. 무료 평가판 기간이 만료되면 자동으로 유료 구독으로 전환됩니다.

무료 평가판 기간이 만료되기 전에 작업 또는 포드를 종료하지 않으면 무료 평가판 기간이 만료될 때 시간당 소프트웨어 요금이 발생합니다. 무료 평가판 구독을 취소해도 작업 또는 포트가 자동으로 종료되지 않으며, 계속 사용할 경우 소프트웨어 요금이 부과됩니다. 자세한 내용은 Amazon ECS 요금 및 Amazon EKS 요금을 참조하세요.

기계 학습 제품의 무료 평가판

시간당 요금이 적용되는 AWS Marketplace의 일부 기계 학습 제품은 무료 평가판을 제공합니다. 무료 평가판을 구독하면 시간당 소프트웨어 요금 없이 판매자가 설정한 기간 동안 Amazon SageMaker 엔드포인트, 배치 변환 작업 또는 학습 작업을 실행할 수 있습니다. 인프라 비용은 구매자가 부담합니다. 무료 평가판 기간이 만료되면 자동으로 유료 구독으로 전환됩니다.

무료 평가판 기간이 만료되기 전에 Amazon SageMaker 엔드포인트, 배치 변환 작업 또는 학습 작업을 종료하지 않으면 무료 평가판 기간이 만료될 때 시간당 소프트웨어 요금이 발생합니다. 무료 평가판 구독을 취소해도 Amazon SageMaker 엔드포인트, 배치 변환 작업 또는 학습 작업이 자동으로 종료되지 않으며, 계속 사용할 경우 소프트웨어 요금이 부과됩니다. 인프라 요금에 대한 자세한 내용은 Amazon SageMaker 요금을 참조하세요.

SaaS 제품의 무료 평가판

AWS Marketplace의 서비스형 소프트웨어(SaaS) 제품은 무료 평가판을 제공합니다. SaaS 무료 평가판은 자동으로 유료 계약으로 전환되지 않습니다. 무료 평가판이 더 이상 필요 없으면 그대로 만료되도록 두면 됩니다. 자세한 내용은 SaaS 무료 평가판 섹션을 참조하세요.

AWS Marketplace에서 AWS 프리 티어 사용하기

AWS는 신규 Amazon Web Services(AWS) 고객이 클라우드에서 시작할 수 있도록 돕기 위해 프리 티어를 도입했습니다. 프리 티어는 새로운 애플리케이션 실행, 클라우드에 있는 기존 애플리케이션 테스트 또는 AWS 사용 체험 등 클라우드에서 실행하는 모든 작업에 사용할 수 있습니다. 무료 사용 기간이 만료되면(또는 애플리케이션이 프리 티어 사용 한도를 초과하는 경우) 종량제 표준 요금을 지불하게 됩니다. 자세한 내용은 AWS 프리 티어 단원을 참조하십시오.

AWS 프리 티어 고객은 1년 동안 Amazon Elastic Compute Cloud(Amazon EC2)의 무료 AWS Marketplace 소프트웨어를 매달 750시간까지 사용할 수 있습니다. 프리 티어를 시작하려면 AWS Marketplace 단원을 참조하십시오.

AWS Marketplace 구독 제품을 AWS Service Catalog에 추가하기

Service Catalog를 사용하는 조직은 Amazon Web Services(AWS)에서 사용이 승인된 IT 서비스 카탈로그를 생성하고 관리할 수 있습니다. 이러한 IT 서비스에는 가상 머신 이미지, 서버, 소프트웨어 및 데이터베이스에서 멀티 티어 애플리케이션 아키텍처를 완성하는 모든 서비스가 포함될 수 있습니다. Service Catalog를 사용하면 일반적으로 배포되는 IT 서비스를 중앙에서 관리할 수 있습니다. Service Catalog를 사용하면 일관적인 거버넌스를 달성하고 규정 준수 요건을 충족할 수 있으며, 사용자는 승인된 필수 IT 서비스만 빠르게 배포할 수 있습니다.

자세한 내용은 Service Catalog 관리자 안내서의 포트폴리오에 AWS Marketplace 제품 추가를 참조하세요.

제품 리뷰

AWS Marketplace는 구매할 제품을 현명하게 선택하는 데 필요한 정보를 구매자에게 제공하려고 노력하고 있습니다. AWS 고객은 AWS Marketplace에 등록된 품목에 대한 리뷰를 작성하여 제출할 수 있습니다. 좋은 리뷰든 나쁜 리뷰든 적극적으로 공유해 주시기 바랍니다.

> **Note**
>
> 데이터 제품은 제품 리뷰를 지원하지 않습니다.

지침

AWS Marketplace에서 제품을 구독하고 있는 사람이라면 누구든지 제품 리뷰를 작성할 수 있습니다. 제품 리뷰를 작성하는 경우 다음 지침을 사용하십시오.

- 이유 기재 - 제품에 대한 호불호 뿐만 아니라 이유까지도 리뷰에 포함되어야만 가장 효과적인 리뷰가 될 수 있습니다. 관련 제품을 비롯해 리뷰 제품과 관련 제품의 비교 방법에 대해서도 작성해주십시오.
- 구체적으로 작성 - 리뷰는 제품의 특정 기능과 제품에 대한 사용자 경험을 중심으로 작성되어야 합니다. 동영상 리뷰일 때는 간략한 소개도 작성하는 것이 좋습니다.
- 간결하게 작성 - 리뷰는 20~5,000자 사이여야 합니다. 적당한 길이는 75~500자입니다.
- 진정성 - 긍정적 의견이든 부정적 의견이든, 제품에 대한 솔직한 의견을 보내주시면 감사하겠습니다. 유용한 정보는 모두 고객의 구매 결정에 영향을 미칠 수 있습니다.
- 투명성 - 리뷰 대가로 무료 제품을 받았다면 제품을 무료로 받았다고 누구나 알 수 있게, 그리고 명확하게 공개하세요.

제한 사항

AWS는 다음 콘텐츠 중 하나를 포함하는 리뷰를 삭제할 권리를 보유합니다.

- 다음을 포함하여 객관적인 자료:
  - 음란하거나 혐오스러운 콘텐츠
  - 모욕적이거나 악의적인 표현
  - 불법적이거나 부도덕한 행위의 조장

- 다음을 포함하여 프로모션 콘텐츠:
  - 광고, 홍보 자료 또는 동일한 내용을 지나칠 정도로 반복하는 글
  - 해당 제품 또는 직접 경쟁 제품에 대해 금전적인 이권을 가지고 있는 사람 또는 회사가 작성하거나, 혹은 그러한 사람 또는 회사를 대신해 작성하는 리뷰(저자, 게시자, 제조사 또는 해당 제품을 판매하는 제3의 상사가 작성하는 리뷰 포함)
  - 유료 홍보 패키지의 일부인 리뷰를 포함하여 상품의 무료 사본 이외의 모든 형태의 보상을 위해 작성된 리뷰
  - 입증할 수 있는 제품 구독이 없는 고객이 작성한 리뷰
- 다음을 포함하여 부적절한 콘텐츠:
  - 과도한 견적을 포함하여 기타 매체에서 복사한 콘텐츠
  - Amazon.com 외부 연락처 정보 또는 URL
  - 가용성 또는 대체 주문/배송에 대한 세부 정보
  - 워터마크가 있는 동영상
  - 페이지에 표시되는 의견 또는 기타 리뷰(페이지에 표시되는 의견 또는 기타 리뷰는 사전 공지 없이 변경될 수 있기 때문입니다)
  - 외국어 콘텐츠(제품에 대한 명확한 연관이 있을 때까지)
  - 서식 문제가 있는 텍스트
- 다음을 포함하여 주제를 벗어난 정보:
  - 판매자에 대한 피드백 또는 배송 경험
  - 카탈로그 또는 제품 설명의 오타나 부정확성에 대한 피드백(제품 페이지 하단에 있는 피드백 양식 사용)

고객 리뷰에 대한 질문은 당사에 문의하십시오.

시간 및 기대

저희는 최대한 빠르게 제품 리뷰를 처리할 수 있도록 노력하고 있습니다. 하지만 AWS Marketplace 팀은 리뷰어와 판매자의 의견을 모두 듣고 피드백이 the section called “지침” 및 the section called “제한 사항”와 비교하여 타당한지 확인하고 검토해야 합니다. 프로세스를 완료하는 데 걸리는 시간은 AWS Marketplace 판매자 설명서에 설명된 것과 동일한 시간 및 기대 지침을 따릅니다.

지원 받기

일반적인 AWS Marketplace 문제는 AWS에 문의하세요. AWS Marketplace에서 구매한 소프트웨어 문제일 때는 해당 소프트웨어 판매자에게 문의하십시오.

AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights는 신뢰할 수 있고 산업 표준을 충족하는 소프트웨어를 조달할 수 있도록 지원함으로써 소프트웨어 위험 평가를 간소화합니다. AWS Marketplace Vendor Insights를 사용하면 단일 사용자 인터페이스에서 제품의 보안 프로필을 거의 실시간으로 모니터링할 수 있습니다. 또한 소프트웨어 제품의 보안 정보에 대한 대시보드를 제공하여 평가 부담을 줄여줍니다. 이 대시보드를 사용하여 데이터 프라이버시, 애플리케이션 보안, 액세스 제어와 같은 정보를 살펴보고 평가할 수 있습니다.

AWS Marketplace Vendor Insights는 산업 표준을 지속적으로 충족하는 신뢰할 수 있는 소프트웨어를 조달하여 판매자로부터 보안 데이터를 수집하고 구매자를 지원합니다. AWS Marketplace Vendor Insights는 AWS Audit Manager와 통합하면 AWS Marketplace의 서비스형 소프트웨어(SaaS) 제품에 대한 최신 보안 정보를 자동으로 가져올 수 있습니다. AWS Marketplace Vendor Insights는 AWS Artifact 서드 파티 보고서와 통합되므로 AWS 서비스에 대한 보고서와 함께 공급업체 소프트웨어에 대한 온디맨드 규정 준수 보고서에 액세스할 수 있습니다.

AWS Marketplace Vendor Insights는 10개 제어 범주와 여러 컨트롤의 증거 기반 정보를 제공합니다. 또한 다음 세 가지 소스에서 증거 기반 정보를 수집합니다.

- 공급업체 프로덕션 계정 - 여러 컨트롤 중에서 25개 컨트롤은 공급업체의 프로덕션 계정에서 실시간으로 증거를 수집할 수 있도록 지원합니다. 각 컨트롤에 대한 실시간 증거는 판매자의 AWS 리소스 구성 설정을 평가하는 하나 이상의 AWS Config 규칙에 의해 생성됩니다. 실시간 증거는 여러 소스의 데이터를 지속적으로 업데이트하여 최신 정보를 제공하는 방법입니다. AWS Audit Manager는 증거를 캡처하여 AWS Marketplace Vendor Insights 대시보드에 전달합니다.
- Vendor ISO 27001 및 SOC 2 Type II 보고서 - 컨트롤 범주는 국제 표준화 기구(ISO) 및 SOC(Service Organization Control) 2 보고서의 규제 항목에 매핑됩니다. 판매자가 이러한 보고서를 AWS Marketplace Vendor Insights와 공유하면 Vendor Insights는 관련 데이터를 추출하여 대시보드에 표시합니다.
- 공급업체 자체 평가 - 판매자는 자체 평가를 완료합니다. 또한 AWS Marketplace Vendor Insights 보안 자체 평가 및 CAIQ(Consensus Assessment Initiative Questionnaire)를 비롯한 기타 자체 평가 유형을 생성하여 업로드할 수도 있습니다.

다음 비디오는 SaaS 위험 평가를 간소화하고 AWS Marketplace Vendor Insights를 사용하는 방법을 보여줍니다.

구매자로 AWS Marketplace Vendor Insights 시작하기

AWS Marketplace Vendor Insights는 AWS Marketplace에 제공되는 소프트웨어 제품에 대한 보안 정보를 제공합니다. AWS Marketplace Vendor Insights를 사용하여 AWS Marketplace에 있는 제품의 보안 프로필을 볼 수 있습니다.

AWS Marketplace Vendor Insights 대시보드에는 AWS Marketplace Vendor Insights를 사용하여 제품을 평가하는 소프트웨어 제품에 대한 규정 준수 아티팩트 및 보안 컨트롤 정보가 표시됩니다. AWS Marketplace Vendor Insights는 이 대시보드에 표시되는 여러 보안 컨트롤에 대한 증거 기반 정보를 수집합니다.

AWS Marketplace Vendor Insights를 사용하여 제품의 보안 및 규정 준수 정보에 액세스하는 것은 무료입니다.

AWS Marketplace Vendor Insights에서 제품을 찾아보세요.

AWS Marketplace Vendor Insights 대시보드에서 제품의 프로필과 요약 정보를 볼 수도 있고, 범주 컨트롤을 선택하여 제품에 수집된 데이터에 대해 자세히 알아볼 수도 있습니다. AWS Marketplace Vendor Insights에서 AWS Marketplace의 제품을 찾으려면 다음 절차를 수행합니다.

AWS Marketplace Vendor Insights에서 제품을 찾는 방법

1. AWS Management Console에 로그인한 다음 AWS Marketplace 콘솔을 엽니다.
2. 모든 제품 보기를 선택합니다.
3. Vendor Insights 태그가 있는 제품을 봅니다.
4. Vendor Insights의 결과 구체화에서 보안 프로필을 선택합니다.
5. 제품 세부 정보 페이지의 제품 개요에서 Vendor Insights 섹션을 선택합니다.
6. 이 제품의 모든 프로필 보기를 선택합니다.
7. 개요에서 제품 세부 정보와 받은 보안 인증서 목록을 볼 수 있습니다.
8. 액세스 요청을 선택합니다.
9. Vendor Insight 데이터에 대한 액세스 권한 요청 페이지에서 자신의 정보를 입력하고 액세스 요청을 선택합니다.

   이 제품의 AWS Marketplace Vendor Insights 데이터에 대한 액세스 권한을 성공적으로 요청했다는 내용의 성공 메시지가 나타납니다.

구독하여 평가 데이터에 대한 액세스 권한 요청

AWS Marketplace Vendor Insights에서 공급업체 소프트웨어의 보안 프로필을 지속적으로 모니터링할 수 있습니다. 먼저 모니터링하려는 제품에 대한 공급업체 평가 데이터를 구독하거나 액세스 권한을 요청합니다. 제품에 대한 평가 데이터를 더 이상 모니터링할 필요가 없으면 평가 데이터를 구독 해지할 수 있습니다. AWS Marketplace Vendor Insights를 사용하여 제품의 보안 및 규정 준수 정보에 액세스하는 것은 무료입니다. 요금에 대한 자세한 내용은 AWS Marketplace Vendor Insights 요금을 참조하세요.

특정 공급업체 제품에 대한 모든 평가 데이터에 액세스하려면 해당 제품의 평가 데이터를 구독해야 합니다.

제품에 대한 AWS Marketplace Vendor Insights 평가 데이터를 구독하는 방법

1. AWS Management Console에 로그인한 다음 AWS Marketplace 콘솔을 엽니다.
2. Vendor Insights를 선택합니다.
3. Vendor Insights에서 제품을 선택합니다.
4. Overview(개요) 탭을 선택합니다.
5. 액세스 요청을 선택합니다.
6. 나머지 필드에 정보를 입력합니다.
7. 모두 마쳤으면 액세스 요청을 선택합니다.

   이 제품의 모든 공급업체 평가 데이터에 대한 액세스 권한을 요청했다는 내용의 성공 메시지가 나타납니다.

평가 데이터 구독 해지

공급업체 제품에 대한 평가 데이터에 더 이상 액세스할 필요가 없으면 제품의 평가 데이터를 구독 해지할 수 있습니다.

제품에 대한 AWS Marketplace Vendor Insights 평가 데이터를 구독 해지하는 방법

1. AWS Management Console에 로그인한 다음 AWS Marketplace 콘솔을 엽니다.
2. Vendor Insights를 선택합니다.
3. 제품 세부 정보 페이지에서 제품을 선택하고 구독 해지를 선택합니다.
4. AWS Marketplace Vendor Insights 데이터를 구독 해지하면 제공되는 약관을 읽어봅니다.

5. 텍스트 입력 필드에 **Unsubscribe**를 입력하고 구독 해지를 선택합니다.

   AWS Marketplace Vendor Insights 데이터를 구독 해지했으며 액세스 요금이 더 이상 부과되지 않는다는 내용의 성공 메시지가 나타납니다.

AWS Marketplace Vendor Insights에서 제품의 보안 프로필 보기

AWS Marketplace Vendor Insights는 판매자로부터 보안 데이터를 수집합니다. 제품의 보안 프로필에는 제품의 보안, 복원력, 규정 준수 및 평가에 필요한 기타 요소에 대한 업데이트된 정보가 표시됩니다. 이 정보는 산업 표준을 지속적으로 준수하는 신뢰할 수 있는 소프트웨어를 조달할 수 있도록 지원함으로써 구매자를 지원합니다. AWS Marketplace Vendor Insights는 평가하는 각 서비스형 소프트웨어(SaaS) 제품의 여러 보안 컨트롤에 대한 증거 기반 정보를 수집합니다.

주제

- AWS Marketplace Vendor Insights의 대시보드
- SaaS 제품의 보안 프로필 보기
- 컨트롤 범주 이해

AWS Marketplace Vendor Insights의 대시보드

이 대시보드에는 AWS Marketplace Vendor Insights가 수집한 소프트웨어 제품에 대한 규정 준수 아티팩트 및 보안 컨트롤 정보가 표시됩니다. 데이터 레지던시 변경 또는 인증 만료와 같은 모든 보안 컨트롤 범주에 대한 증거 기반 정보가 제공됩니다. 통합 대시보드는 규정 준수 정보 변경 사항을 제공합니다. AWS Marketplace Vendor Insights를 사용하면 추가 설문지를 작성하고 위험 평가 소프트웨어를 사용할 필요가 없습니다. 대시보드가 지속적으로 업데이트 및 검증되므로 소프트웨어를 조달한 후에도 소프트웨어의 보안 컨트롤을 지속적으로 모니터링할 수 있습니다.

SaaS 제품의 보안 프로필 보기

AWS Marketplace Vendor Insights는 판매자의 소프트웨어에 대한 결정을 내리는 데 도움이 됩니다. AWS Marketplace Vendor Insights는 10개 컨트롤 범주와 여러 컨트롤에 걸쳐 판매자의 증거 기반 정보에서 데이터를 추출합니다. 대시보드에서 SaaS 제품의 프로파일 및 요약 정보를 확인하거나, 컨트롤 범주를 선택하여 수집된 데이터에 대해 자세히 알아볼 수 있습니다. 프로파일을 통해 규정 준수 정보를 보려면 제품을 구독하고 액세스 권한을 부여받아야 합니다.

1. AWS Management Console에 로그인하고 AWS Marketplace 콘솔을 엽니다.
2. Vendor Insights를 선택합니다.

3. Vendor Insights에서 제품을 선택합니다.
4. 프로필 세부 정보 페이지에서 보안 및 규정 준수 탭을 선택합니다.

> **Note**
>
> 빨간색 원 안의 숫자는 규정을 준수하지 않는 컨트롤의 수를 나타냅니다.

5. 컨트롤 범주의 경우 나열된 범주 중 하나에서 텍스트를 선택하면 자세한 내용을 볼 수 있습니다.

   - 첫 번째 컨트롤 이름을 선택합니다(해당 법률, 규제 및 계약 요구 사항을 준수하도록 보장하는 정책/절차가 있습니까?).
   - 표시된 정보를 읽습니다. AWS Artifact 타사 보고서의 보고서를 보거나 감사자의 예외를 볼 수도 있습니다.
   - 제품 세부 정보 페이지로 돌아가려면 위의 탐색 메뉴에서 제품 이름을 선택합니다.

컨트롤 범주 이해

AWS Marketplace Vendor Insights는 10개 컨트롤 범주 내 여러 컨트롤의 증거 기반 정보를 제공합니다. AWS Marketplace Vendor Insights는 공급업체 프로덕션 계정, 공급업체 자체 평가, 공급업체 ISO 27001 및 SOC 2 Type II 보고서라는 세 가지 소스에서 정보를 수집합니다. 세 가지 리소스에 대한 자세한 내용은 AWS Marketplace Vendor Insights 섹션을 참조하세요.

다음 목록은 각 컨트롤 범주에 대한 설명을 제공합니다.

액세스 관리

시스템 또는 애플리케이션에 대한 액세스를 식별, 추적, 관리 및 제어합니다.

애플리케이션 보안

애플리케이션을 설계, 개발 및 테스트할 때 애플리케이션에 보안이 통합되었는지 확인합니다.

감사, 규정 준수 및 보안 정책

조직이 규제 요구 사항을 준수하는지 평가합니다.

비즈니스 복원력 및 연속성

비즈니스 연속성을 유지하면서 시스템 중단에 빠르게 대응하는 조직의 능력을 평가합니다.

데이터 보안

데이터 및 자산을 보호합니다.

최종 사용자 디바이스 보안

휴대용 최종 사용자 디바이스 및 이러한 디바이스가 연결된 네트워크를 위협과 취약성으로부터 보호합니다.

인적 자원

직원 채용, 급여 지급, 계약 종료 등의 프로세스 중에 민감한 데이터를 처리하는 직원 관련 부서를 평가합니다.

인프라 보안

중요 자산을 위협과 취약성으로부터 보호합니다.

위험 관리 및 인시던트 대응

수용 가능한 것으로 간주되는 위험 수준과 위험 및 공격에 대응하기 위해 수행된 조치를 평가합니다.

보안 및 구성 정책

조직의 자산을 보호하는 보안 정책 및 보안 구성을 평가합니다.

컨트롤 범주 세트

다음 표에는 수집한 각 범주의 값에 대한 정보와 함께 각 범주에 대한 구체적인 정보가 나와 있습니다. 다음 목록에는 표의 각 열에 있는 정보 유형이 설명되어 있습니다.

- 컨트롤 세트 - 컨트롤은 컨트롤 세트에 할당되며, 각 컨트롤은 해당 범주의 보안 기능을 반영합니다. 각 범주에는 여러 컨트롤 세트가 있습니다.
- 컨트롤 이름 - 정책 또는 절차의 이름입니다. “수동 증명 필요”는 정책 또는 절차에 대한 서면 확인서 또는 문서가 필요하다는 뜻입니다.
- 컨트롤 설명 - 이 정책 또는 절차에 필요한 질문, 정보 또는 문서입니다.
- 증거 추출 세부 정보 - 이 범주에 필요한 데이터를 추가로 확보하려면 있어야 하는 컨트롤에 대한 정보 및 컨텍스트입니다.
- 샘플 값 - 규제 표준을 충족하려면 이 범주의 규정 준수 값이 어떻게 되어야 하는지 지침을 제공하는 예제입니다.

주제

- 액세스 관리 컨트롤
- 애플리케이션 보안 컨트롤
- 감사 및 규정 준수 컨트롤
- 비즈니스 복원력 컨트롤
- 데이터 보안 컨트롤
- 최종 사용자 디바이스 보안 컨트롤
- 인적 자원 컨트롤
- 인프라 보안 컨트롤
- 위험 관리 및 인시던트 대응 컨트롤
- 보안 및 구성 정책 컨트롤

액세스 관리 컨트롤

액세스 관리 컨트롤은 시스템 또는 애플리케이션에 대한 액세스를 식별, 추적, 관리 및 제어합니다. 이 표에는 액세스 관리 컨트롤의 값과 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명
보안 인증	액세스 관리 3.1.1 - 보안 인증 - UserId의 개인 데이터(수동 증명 필요)	사용자 ID에 이름 또는 이메일 주소터가 필요한가요?
	액세스 관리 3.1.2 - 보안 인증 - 애플리케이션에서 2단계 인증 지원(수동 증명 필요)	애플리케이션이 2단계 인증을 지원
	액세스 관리 3.1.3 - 보안 인증 - 계정 잠금(수동 증명 필요)	고객이 로그인에 여러 번 실패하면 요?
보안 인증 정보 관리	액세스 관리 3.2.1 - 보안 인증 정보 관리 - 암호 정책	애플리케이션에 강력한 암호 정책이

컨트롤 세트	컨트롤 제목	컨트롤 설명
	액세스 관리 3.2.2 - 보안 인증 정보 관리 - 암호 암호화	로그인 보안 인증 정보(암호 및 사용 암호화하고 저장 시 솔트로 해시하 요구하나요?
	액세스 관리 3.2.3 - 보안 인증 정보 관리 - 보안 암호 관리	보안 암호 관리 서비스를 사용하시
	액세스 관리 3.2.4 - 보안 인증 정보 관리 - 코드의 보안 인증 정보(수동 증명 필요)	코드에 보안 인증 정보가 포함되나
프로덕션 환경 액세스	액세스 관리 3.3.1 - 프로덕션 환경 액세스 - Single Sign-on(수동 증명 필요)	프로덕션 환경에 액세스할 때 SSO
	액세스 관리 3.3.2 - 프로덕션 환경 액세스 - 2단계 인증	프로덕션 또는 호스팅 환경에 액세 증이 필요한가요?
	액세스 관리 3.3.3 - 프로덕션 환경 액세스 - 루트 사용자(수동 증명 필요)	루트 사용자는 프로덕션 환경에 액 으로 사용되나요?
	액세스 관리 3.3.4 - 프로덕션 환경 액세스 - 루트 사용자 MFA	루트 사용자는 다중 인증(MFA)이 필
	액세스 관리 3.3.5 - 프로덕션 환경 액세스 - 원격 액세스	암호화된 채널 또는 키 기반 인증과 사용하여 프로덕션 환경에 대한 원 나요?
액세스 제어 정책	액세스 관리 3.4.1 - 액세스 제어 정책 - 최소 권한 액세스	사용자가 프로덕션 환경에 액세스할 스 정책을 따르나요?

컨트롤 세트	컨트롤 제목	컨트롤 설명
	액세스 관리 3.4.2 - 액세스 제어 정책 - 액세스 정책 검토	프로덕션 환경의 모든 액세스 정책 하나요?
	액세스 관리 3.4.3 - 액세스 제어 정책 - 사용자 및 보안 정책 구성(수동 증명 필요)	고객이 사용자 및 사용자의 권한을 애플리케이션에서 허용하나요?
	액세스 관리 3.4.4 - 액세스 제어 정책 - 논리적 세분화(수동 증명 필요)	애플리케이션 사용자를 논리적으로
	액세스 관리 3.4.5 - 액세스 제어 정책 - 계약 종료 시 액세스 권한 검토	직원 계약 종료 또는 역할 변경 시 책을 업데이트하나요?
액세스 로그	액세스 제어 3.5.1 - 액세스 로그	프로덕션 환경에서 개별 사용자가 하나요?

애플리케이션 보안 컨트롤

애플리케이션 보안 컨트롤은 애플리케이션을 설계, 개발 및 테스트할 때 애플리케이션에 보안이 통합되었는지 확인합니다. 이 표에는 애플리케이션 보안 정책 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
보안 소프트웨어 개발 수명 주기	애플리케이션 보안 4.1.1 - 보안 소프트웨어 개발 수명 주기 - 별도의 환경	개발, 테스트 및 스테이징 환경이 프로덕션 환경과 분리되어 있나요?	개발, 테스트 및 스테이징 환경이 프로덕션 환경과 분리되는지 지정합니다.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	애플리케이션 보안 4.1.2 - 보안 소프트웨어 개발 수명 주기 - 안전한 코딩 수칙	보안 엔지니어가 개발자와 함께 보안 수칙을 연구하나요?	개발자와 보안 엔지니어가 협력하여 안전한 코딩 수칙을 연구하는지 지정합니다.	예
	애플리케이션 보안 4.1.3 - 보안 소프트웨어 개발 수명 주기 - 테스트 환경에서 고객 데이터 사용(수동 증명 필요)	고객 데이터를 테스트, 개발 또는 QA 환경에서 사용한 적이 있나요?	고객 데이터를 테스트, 개발 또는 QA 환경에서 사용한 적이 있나요? 그렇다면, 어떤 데이터를 어떤 목적으로 사용했나요?	아니요
	애플리케이션 보안 4.1.4 - 보안 소프트웨어 개발 수명 주기 - 보안 연결	고객 데이터를 사용하는 모든 웹 페이지 및 통신에 SSL/TLS를 사용하나요?	고객 데이터와의 모든 통신에 보안 연결(예: SSL/TLS)을 사용할 것인지 지정합니다.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	애플리케이션 보안 4.1.5 - 보안 소프트웨어 개발 수명 주기 - 이미지 백업	애플리케이션 이미지 스냅샷이 백업되나요?	이미지 스냅샷(예: 애플리케이션을 지원하는 시스템 및 고객 데이터를 호스팅하는 시스템)을 백업할 것인지 지정합니다. 그렇다면, 범위가 지정된 데이터를 포함하는 이미지 스냅샷을 만들기 전에 인가를 받도록 하는 프로세스가 있나요? 이미지 스냅샷에 대한 액세스 제어가 구현되어 있나요?	예. 이미지는 고객과 경영진의 승인을 받아 백업됩니다.
애플리케이션 보안 검토	애플리케이션 보안 4.2.1 - 애플리케이션 보안 검토 - 보안 코드 검토	각 릴리스 전에 보안 코드 검토를 수행하나요?	각 릴리스 전에 보안 코드 검토를 수행할 것인지 지정합니다.	예
	애플리케이션 보안 4.2.2 - 애플리케이션 보안 검토 - 침투 테스트	침투 테스트를 수행하나요? 침투 테스트 보고서를 받을 수 있나요?	애플리케이션에서 침투 테스트를 수행할 것인지 지정합니다. 그렇다면, 최근 보고서 3개를 수동 증거로 공유해 주실 수 있나요?	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	애플리케이션 보안 4.2.3 - 애플리케이션 보안 검토 - 보안 패치	사용 가능한 모든 고위험 보안 패치를 정기적으로 적용하고 검증하나요?	고위험 보안 패치를 정기적으로 적용할 것인지 지정합니다. 그렇다면, 얼마나 자주 적용하나요?	예. 보안 패치는 매월 적용됩니다.
	애플리케이션 보안 4.2.4 - 애플리케이션 보안 검토 - 애플리케이션의 취약성 검사	모든 인터넷 연결 애플리케이션의 취약성을 정기적으로 그리고 중대한 변경 후에 검사하나요?	모든 인터넷 연결 애플리케이션에서 취약성 검사를 수행할 것인지 지정합니다. 그렇다면, 취약성 검사를 얼마나 자주 하나요? 보고서 사본을 받을 수 있나요?	예. 취약성 검사는 매월 수행됩니다.
	애플리케이션 보안 4.2.5 - 애플리케이션 보안 검토 - 위협 및 취약성 관리	위협 및 취약성 평가 도구와 이러한 도구가 수집한 데이터를 관리하는 프로세스가 있나요?	위협 및 취약성 평가 도구와 이러한 도구가 수집한 데이터를 관리하는 프로세스가 있는지 지정합니다. 위협 및 취약성을 관리하는 방법에 대해 자세히 설명해 주세요.	예. 다양한 소스의 모든 위협 및 취약성이 하나의 포털에 집계됩니다. 위협 및 취약성은 심각도에 따라 관리됩니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	애플리케이션 보안 4.2.6 - 애플리케이션 보안 검토 - 맬웨어 방지 검사	애플리케이션을 호스팅하는 네트워크 및 시스템에 대한 맬웨어 방지 검사를 정기적으로 수행하나요?	애플리케이션을 호스팅하는 네트워크 및 시스템에 대한 맬웨어 방지 검사를 수행할 것인지 지정합니다. 그렇다면, 얼마나 자주 수행하나요? 보고서를 제공해 주실 수 있나요?	예. 맬웨어 방지 검사는 매월 수행됩니다.
애플리케이션 로그	애플리케이션 보안 4.3.1 - 애플리케이션 로그 - 애플리케이션 로그	애플리케이션 로그를 수집하고 검토하나요?	애플리케이션 로그를 수집하고 검토할 것인지 지정합니다. 그렇다면, 로그를 얼마나 오래 유지하나요?	예. 로그는 1년 동안 보존됩니다.
	애플리케이션 보안 4.3.2 - 애플리케이션 로그 - 로그 액세스	운영 체제 및 애플리케이션 로그가 수정, 삭제 또는 부적절한 액세스로부터 보호되나요?	운영 체제 및 애플리케이션 로그를 수정, 삭제 또는 부적절한 액세스로부터 보호할 것인지 지정합니다. 침해나 인시던트 발생 시 애플리케이션 로그의 손실을 감지할 수 있는 프로세스가 마련되어 있나요?	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	애플리케이션 보안 4.3.3 - 애플리케이션 로그 - 로그에 저장된 데이터(수동 증명 필요)	고객의 개인 식별 정보(PII)를 로그에 저장하나요?	고객의 개인 식별 정보(PII)를 로그에 저장할 것인지 지정합니다.	아니요. PII 데이터를 로그에 저장하지 않습니다.
변경 제어 정책	애플리케이션 보안 4.4.1 - 변경 제어 정책 - 기능 및 복원력 테스트	변경 사항을 릴리스하기 전에 기능 및 복원력 테스트를 수행하나요?	새 릴리스 전에 애플리케이션에서 기능 및 복원력 테스트를 수행할 것인지 지정합니다.	예
	애플리케이션 보안 4.4.2 - 변경 제어 정책 - 변경 제어 절차	프로덕션 환경의 모든 변경 사항에 변경 제어 절차가 필요한가요?	프로덕션 환경에서 이루어지는 모든 변경 사항에 변경 제어 절차를 적용할 것인지 지정합니다.	예
	애플리케이션 보안 4.4.3 - 변경 제어 정책 - 프로덕션 환경에서 인적 오류 및 위험 방지	인적 오류와 위험이 프로덕션 환경에 영향을 미치지 않도록 확인하는 프로세스를 갖추고 있나요?	인적 오류와 위험이 프로덕션 환경에 영향을 미치지 않도록 확인하는 프로세스가 있는지 지정합니다.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	애플리케이션 보안 4.4.4 - 변경 제어 정책 - 변경 사항 문서화 및 로깅	서비스에 영향을 미칠 수 있는 변경 사항을 문서화하고 로깅하나요?	서비스에 영향을 미치는 변경 사항을 문서화하고 로깅할 것인지 지정합니다. 그렇다면, 로그를 얼마나 오래 유지하나요?	예
	애플리케이션 보안 4.4.5 - 변경 제어 정책 - 구매자를 위한 변경 알림(수동 증명 필요)	고객의 서비스에 영향을 미칠 수 있는 변경 작업을 수행하기 전에 고객에게 알리도록 하는 공식 절차가 있나요?	고객의 서비스에 영향을 미칠 수 있는 변경 작업을 수행하기 전에 고객에게 알릴 것인지 지정합니다. 그렇다면, 영향을 미치는 변경 사항에 대해 고객에게 알리는 SLA는 무엇입니까?	예. 변경 사항을 적용하기 90일 전에 고객에게 알립니다.

감사 및 규정 준수 컨트롤

감사 및 규정 준수 컨트롤은 조직이 규제 요구 사항을 준수하는지 평가합니다. 이 표에는 감사 및 규정 준수 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
완료된 인증	감사 및 규정 준수 1.1.1 - 완료된 인증(수동 증명 필요)	보유한 인증서를 기재합니다.	보유한 인증서를 명시합니다.	SOC2, ISO/IEC 27001

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
진행 중인 인증	감사 및 규정 준수 1.2.1 - 진행 중인 인증(수동 증명 필요)	현재 진행 중인 추가 인증을 기재합니다.	현재 감사 또는 검토 중인 추가 인증을 예상 완료 날짜와 함께 기재합니다.	예. PCI 인증이 진행 중입니다(예상 완료 시간은 2022년 2분기).
규정 준수를 보장하는 절차	감사 및 규정 준수 1.3.1 - 규정 준수를 보장하는 절차 - 규정 준수를 보장하는 절차	해당하는 법률, 규제 및 계약 요구 사항을 준수하도록 보장하는 정책 또는 절차가 있나요?	해당하는 법률, 규제 및 계약 요구 사항을 준수하도록 보장하는 정책 또는 절차가 있는지 지정합니다. 그렇다면, 절차에 대한 세부 정보를 기재하고 수동 증거를 업로드하세요.	예. SOC2, ISO/IEC 27001과 같은 문서를 업로드했습니다.
	감사 및 규정 준수 1.3.2 - 규정 준수를 보장하는 절차 - 미해결 요구 사항을 추적하기 위한 감사	미해결 규제 및 규정 준수 요구 사항을 추적하기 위한 감사를 수행하나요?	미해결 요구 사항을 추적하기 위한 감사를 수행하는지 지정합니다. 그렇다면, 세부 정보를 입력하세요.	미해결 요구 사항을 추적하기 위한 감사를 매월 수행합니다.
	감사 및 규정 준수 1.3.3 - 규정 준수를 보장하는 절차 - 편차 및 예외(수동 증명 필요)	규정 준수 요구 사항과 다른 편차 및 예외를 처리하는 프로세스가 있나요?	규정 준수 요구 사항과 다른 편차 및 예외를 처리하는 프로세스가 있는지 지정합니다. 그렇다면, 세부 정보를 입력하세요.	예. 편차 로그 및 보고 도구가 있습니다. 향후 재발을 방지하기 위해 모든 예외 또는 편차를 조사합니다.

비즈니스 복원력 컨트롤

비즈니스 복원력 컨트롤은 비즈니스 연속성을 유지하면서 시스템 중단에 빠르게 대응하는 조직의 능력을 평가합니다. 이 표에는 비즈니스 복원력 정책 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
비즈니스 복원력	비즈니스 복원력 및 연속성 6.1.1 - 비즈니스 복원력 - 장애 조치 테스트(수동 증명 필요)	사이트 장애 조치 테스트를 적어도 1년에 한 번 수행하나요?	장애 조치 테스트를 매년 수행할 것인지 지정합니다. 그렇지 않다면, 얼마나 자주 수행하나요?	예
	비즈니스 복원력 및 연속성 6.1.2 - 비즈니스 복원력 - 비즈니스 영향 분석(수동 증명 필요)	비즈니스 영향 분석을 수행했나요?	비즈니스 영향 분석을 수행했는지 지정합니다. 그렇다면, 언제 마지막으로 완료했나요? 수행한 분석에 대한 세부 정보를 입력하세요.	예. 비즈니스 영향 분석은 6개월 전에 완료되었습니다.
	비즈니스 복원력 및 연속성 6.1.3 - 비즈니스 복원력 - 타사 공급업체에 대한 종속성(수동 증명 필요)	중요한 타사 서비스 공급자(클라우드 서비스 공급자 제외)에게 종속되어 있나요?	타사 공급업체(클라우드 서비스 공급자 제외)에 종속되어 있는지 지정합니다. 그렇다면, 공급업체에 대한 세부 정보를 제공해 주실 수 있나요?	아니요
	비즈니스 복원력 및 연속성 6.1.4 - 비즈니스 복원력 - 타사 연속성 및	타사 공급업체가 자체적인 재해 복구 프로세스 및	타사 공급업체가 자체적인 재해 복구 프로세스 및 활동을 보유하고	이 샘플에는 해당하지 않습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	복구 테스트(수동 증명 필요)	활동을 보유하고 있어야 하나요?	있어야 하는지 지정합니다.	
	비즈니스 복원력 및 연속성 6.1.5 - 비즈니스 복원력 - 타사 공급업체 계약 위반(수동 증명 필요)	중요 서비스 공급자와 맺은 계약에 SSA(Sold and Shipped by Amazon) 가용성 및 연속성 위반에 대한 위약금 또는 구제 조항이 포함되어 있나요?	타사 공급업체와 맺은 계약에 가용성 및 연속성 위반에 대한 위약금 또는 구제 조항이 포함되어 있나요?	이 샘플에는 해당하지 않습니다.
	비즈니스 복원력 및 연속성 6.1.6 - 비즈니스 복원력 - 시스템 상태	시스템 상태를 파악할 수 있는 모니터나 알림이 있나요?	시스템 상태를 파악할 수 있는 모니터 또는 알림이 있는지 지정합니다.	예
비즈니스 연속성	비즈니스 복원력 및 연속성 6.2.1 - 비즈니스 연속성 - 비즈니스 연속성 정책 및 절차	공식적인 비즈니스 연속성 절차를 개발하고 문서화했나요?	비즈니스 연속성을 위한 공식 절차를 개발하여 유지하고 있는지 지정합니다. 그렇다면, 절차에 대한 자세한 내용을 입력하세요.	예
	비즈니스 탄력성 및 연속성 6.2.2 - 비즈니스 연속성 - 대응 및 복구 전략	우선 순위가 지정된 활동에 대한 구체적인 대응 및 복구 전략이 정의되어 있나요?	고객 활동 및 서비스에 대한 복구 및 대응 전략을 개발했는지 지정합니다.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	비즈니스 복원력 및 연속성 6.2.3 - 비즈니스 연속성 - 비즈니스 연속성 테스트	비즈니스 연속성을 보장하기 위한 복구 테스트를 수행하나요?	장애 발생 시 비즈니스 연속성을 보장하기 위해 복구 테스트를 수행하는지 지정합니다.	예. 장애 발생 시 비즈니스 연속성을 위해 시스템이 2시간 이내에 활성화됩니다.
	비즈니스 복원력 및 연속성 6.2.4 - 비즈니스 연속성 - 멀티테넌시 환경의 가용성에 미치는 영향(수동 증명 필요)	시스템 내 다른 사용자의 가용성에 영향을 미칠 수 있는 부하를 부과하는 구매자의 능력을 제한하고 있나요?	한 구매자의 부하가 다른 구매자의 가용성에 영향을 미칠 수 있는지 지정합니다. 그렇다면, 영향을 미치지 않는 임계값은 얼마인가요? 그렇지 않다면, 사용량이 가장 많은 시간에 서비스에 영향을 미치지 않도록 어떤 방법을 사용하시는지 자세히 설명해 주세요.	예. 이 샘플은 임계값이 없습니다.
애플리케이션 가용성	비즈니스 복원력 및 연속성 6.3.1 - 애플리케이션 가용성 - 가용성 기록(수동 증명 필요)	작년에 신뢰성 또는 가용성과 관련된 중대한 문제가 있었나요?	작년에 신뢰성 또는 가용성과 관련된 중대한 문제가 있었는지 지정합니다.	아니요

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	비즈니스 복원력 및 연속성 6.3.2 - 애플리케이션 가용성 - 예정된 유지 관리 기간(수동 증명 필요)	예정된 유지 관리 기간에 가동 중지가 발생할 수 있나요?	예정된 유지 관리 기간에 서비스가 중단될 수도 있는지 지정합니다. 그렇다면, 가동 중지 시간은 얼마나 될까요?	아니요
	비즈니스 복원력 및 연속성 6.3.3 - 애플리케이션 가용성 - 온라인 인시던트 포털(수동 증명 필요)	계획된 중단과 예상치 못한 중단에 대해 설명하는 온라인 인시던트 대응 상태 포털이 있나요?	계획된 중단과 예상치 못한 중단에 대해 설명하는 인시던트 상태 포털이 있는지 지정합니다. 그렇다면, 고객이 포털에 액세스하는 방법을 자세히 기재해 주세요. 운영이 중단되고 얼마 후에 포털이 업데이트되나요?	예. 고객이 example.com을 통해 세부 정보에 액세스할 수 있습니다.
	비즈니스 복원력 및 연속성 6.3.4 - 애플리케이션 가용성 - Recovery Time Objective (수동 증명 필요)	구체적인 Recovery Time Objective(RTO)가 있나요?	Recovery Time Objective(RTO)가 있는지 지정합니다. 있다면, RTO를 알려주실 수 있나요?	예, RTO는 2시간입니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	비즈니스 복원력 및 연속성 6.3.5 - 애플리케이션 가용성 - Recovery Point Objective (수동 증명 필요)	구체적인 Recovery Point Objective(RPO)가 있나요?	Recovery Point Objective(RPO)가 있는지 지정합니다. 그렇다면, RPO를 알려주실 수 있나요?	예, RPO는 1주일입니다.

데이터 보안 컨트롤

데이터 보안 컨트롤은 데이터와 자산을 보호합니다. 이 표에는 데이터 보안 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
수집된 고객 데이터	데이터 보안 2.1.1 - 수집된 고객 데이터(수동 증명 필요)	제품 기능에 필요한 고객 데이터 목록을 작성합니다.	사용된 모든 고객 데이터에 대해 설명합니다. 민감한 데이터 또는 기밀 데이터가 사용되는지 지정합니다.	민감한 데이터 또는 기밀 데이터는 사용되지 않습니다. 이 제품은 애플리케이션, 인프라, AWS 서비스 등의 로그와 같이 민감하지 않은 정보만 사용합니다. (AWS CloudTrail, AWS Config, VPC 흐름 로그)
데이터 저장 위치	데이터 보안 2.2.1 - 데이터 저장 위치(수동 증명 필요)	고객 데이터는 어디에 저장되나요? 데이터가 저장되는 국가와 리전을 기재합니다.	데이터가 저장되는 국가 및 리전 목록을 지정합니다.	오하이오(미국), 오리건(미국), 아일랜드(EU)

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
액세스 제어	데이터 보안 2.3.1 - 액세스 제어 - 직원 액세스(수동 증명 필요)	직원이 암호화되지 않은 고객 데이터에 액세스할 수 있나요?	직원이 암호화되지 않은 고객 데이터에 액세스할 수 있는지 지정합니다. 그렇다면, 액세스가 필요한 이유를 간략하게 설명하세요. 그렇지 않다면, 액세스를 제어하는 방법을 간략하게 설명하세요.	아니요. 모든 데이터는 저장 시 암호화됩니다. 직원은 고객 데이터에 액세스할 수 없고, 자신의 사용 현황에 대한 데이터에만 액세스할 수 있습니다.
	데이터 보안 2.3.2 - 액세스 제어 - 모바일 애플리케이션(수동 증명 필요)	고객이 모바일 애플리케이션을 통해 자신의 데이터에 액세스할 수 있나요?	고객이 모바일 애플리케이션을 통해 자신의 데이터에 액세스할 수 있는지 지정합니다. 그렇다면, 세부 정보를 입력하세요. 고객은 어떻게 로그인하나요? 애플리케이션에서 보안 인증 정보를 캐시하나요? 토큰은 얼마나 자주 새로 고침 되나요?	아니요. 모바일 애플리케이션을 사용하여 서비스에 액세스할 수 없습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	데이터 보안 2.3.3 - 액세스 제어 - 데이터가 전송되는 국가(수동 증명 필요)	고객 데이터가 출발지 외부 국가로 전송되나요?	고객 데이터가 출발지 외부 국가로 전송되나요? 그렇다면, 고객 데이터가 전송 또는 수신되는 국가 목록을 지정하세요.	아니요
	데이터 보안 2.3.4 - 액세스 제어 - 타사 공급업체와 데이터 공유 여부(수동 증명 필요)	고객 데이터를 타사 공급업체(클라우드 서비스 공급자 제외)와 공유하나요?	고객 데이터를 타사 공급업체와 공유하나요? 그렇다면, 고객 데이터를 제공하는 타사 공급업체와 해당 국가 또는 리전 목록을 지정하세요.	아니요
	데이터 보안 2.3.5 - 액세스 제어 - 타사 공급업체와 관련된 보안 정책	타사 공급업체가 고객 데이터의 기밀성, 가용성 및 무결성을 유지하도록 하는 정책이나 절차가 마련되어 있나요?	타사 공급업체가 고객 데이터의 기밀성, 가용성 및 무결성을 유지하도록 하는 정책이나 절차가 마련되어 있는지 지정합니다. 그렇다면, 정책 또는 절차에 대한 설명서나 문서를 업로드하세요.	이 샘플에는 해당하지 않습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
데이터 암호화	데이터 보안 2.4.1 - 데이터 암호화 - 유휴 데이터 암호화	모든 유휴 데이터가 암호화되나요?	모든 유휴 데이터가 암호화되는지 지정합니다.	예
	데이터 보안 2.4.2 - 데이터 암호화 - 전송 중 데이터 암호화	모든 데이터가 전송 중에 암호화되나요?	모든 데이터가 전송 중에 암호화되는지 지정합니다.	예
	데이터 보안 2.4.3 - 데이터 암호화 - 강력한 알고리즘(수동 증명 필요)	강력한 암호화 알고리즘을 사용하나요?	강력한 암호화 알고리즘을 사용하나요? 그렇다면, 어떤 암호화 알고리즘(예: RSA, AES 256)을 사용하는지 지정합니다.	예. AES 256은 데이터 암호화에 사용됩니다.
	데이터 보안 2.4.4 - 데이터 암호화 - 고유 암호화 키(수동 증명 필요)	고객이 고유 암호화 키를 생성할 수 있는 기능이 제공되나요?	고객이 자신의 고유 암호화 키를 제공하거나 생성할 수 있나요? 그렇다면, 자세한 내용을 기재하고 증거를 업로드하세요.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	데이터 보안 2.4.5 - 데이터 암호화 - 암호화 키 액세스(수동 증명 필요)	직원이 고객의 암호화 키에 액세스할 수 없도록 차단하나요?	직원이 고객의 암호화 키에 액세스할 수 없도록 차단하는지 지정합니다. 그렇지 않다면, 직원이 고객 키에 액세스할 수 있는 이유를 설명하세요. 그렇다면, 어떤 방법으로 액세스를 제어하는지 설명해 주세요.	예. 암호화 키는 안전하게 저장되고 주기적으로 교체됩니다. 직원은 암호화 키에 액세스할 수 없습니다.
데이터 저장 및 분류	데이터 보안 2.5.1 - 데이터 저장 및 분류 - 데이터 백업	고객 데이터를 백업하나요?	고객 데이터를 백업하는지 지정합니다. 그렇다면, 백업 정책(백업 빈도, 백업 저장 위치, 백업 암호화 및 중복성에 대한 세부 정보 포함)을 설명해 주세요.	예. 3개월마다 백업이 수행됩니다. 백업은 암호화되어 고객 데이터와 동일한 리전에 저장됩니다. 고객의 지원 엔지니어는 백업을 복원할 수 있지만 백업에 들어 있는 데이터는 복원할 수 없습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	데이터 보안 2.5.2 - 데이터 저장 및 분류 - 데이터 액세스 제어 정책	저장된 고객 데이터에 대해 적절한 액세스 제어를 구현하나요? 액세스 제어 정책을 제공해 주세요.	저장된 고객 데이터에 대한 적절한 액세스 제어(예: RBAC)를 구현하는지 지정합니다. 데이터에 대한 액세스를 제어하는 방법에 대한 자세한 내용과 수동 증거를 제공합니다.	예. 최소 권한 액세스 제어를 구현하여 고객 데이터에 대한 액세스를 제한합니다.
	데이터 보안 2.5.3 - 데이터 저장 및 분류 - 트랜잭션 데이터(수동 증명 필요)	고객의 트랜잭션 세부 정보(예: 결제 카드 정보, 트랜잭션을 수행하는 그룹에 대한 정보)가 경계 영역에 저장되나요?	고객의 트랜잭션 세부 정보(예: 결제 카드 정보, 트랜잭션을 수행하는 그룹에 대한 정보)가 경계 영역에 저장되나요? 그렇다면, 경계 영역에 저장해야 하는 이유를 설명하세요.	아니요
	데이터 보안 2.5.4 - 데이터 저장 및 분류 - 정보 분류	법률 또는 규제 요구 사항, 비즈니스 가치, 무단 공개 또는 수정에 대한 민감도에 따라 고객 데이터를 분류하나요?	고객 데이터를 민감도에 따라 분류하는지 지정합니다. 그렇다면, 이 분류에 대한 수동 증거를 업로드하세요.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	데이터 보안 2.5.5 - 데이터 저장 및 분류 - 데이터 세분화(수동 증명 필요)	고객 간 데이터 세분화 및 분리 기능이 제공되나요?	여러 고객의 데이터를 세분화하는지 지정합니다. 그렇지 않다면, 교차 오염으로부터 데이터를 보호하기 위해 사용하는 메커니즘을 설명하세요.	예
데이터 보존	데이터 보안 2.6.1 - 데이터 보존(수동 증명 필요)	데이터를 얼마나 오래 유지하나요?	데이터 보존 기간을 지정합니다. 데이터 분류 및 민감도에 따라 보존 기간이 다른 경우 각 보존 기간에 대한 세부 정보를 제공해 주세요.	6개월
구매자의 구독 취소 후 데이터 보존	데이터 보안 2.6.2 - 클라이언트의 구독 취소 이후 데이터 보존(수동 증명 필요)	구독을 취소한 구매자의 데이터를 얼마나 오래 유지하나요?	구독을 취소한 고객의 데이터 보존 기간을 지정합니다.	3개월

최종 사용자 디바이스 보안 컨트롤

최종 사용자 디바이스 보안 컨트롤은 최종 사용자의 휴대용 디바이스 및 이러한 디바이스가 연결된 네트워크를 위협과 취약성으로부터 보호합니다. 이 표에는 최종 사용자 디바이스 보안 정책 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
자산 및 소프트웨어 인벤토리	최종 사용자 디바이스 보안 7.1.1 - 자산 및 소프트웨어 인벤토리 - 자산 인벤토리	자산 인벤토리 목록이 주기적으로 업데이트되나요?	자산 인벤토리가 유지되는지 지정합니다. 그렇다면, 얼마나 자주 업데이트되나요?	예. 인벤토리는 매주 업데이트됩니다.
	최종 사용자 디바이스 보안 7.1.2 - 자산 및 소프트웨어 인벤토리 - 소프트웨어 및 애플리케이션 인벤토리	범위가 지정된 시스템에 설치된 모든 소프트웨어 플랫폼과 애플리케이션의 인벤토리가 있나요?	설치된 모든 소프트웨어와 애플리케이션의 인벤토리를 유지하는지 지정합니다. 그렇다면, 얼마나 자주 업데이트되나요?	예. 인벤토리는 매주 업데이트됩니다.
자산 보안	최종 사용자 디바이스 보안 7.2.1 - 자산 보안 - 보안 패치	사용 가능한 모든 고위험 보안 패치를 모든 최종 사용자 디바이스에 적어도 한 달에 한 번 적용하고 검증하나요?	모든 고위험 보안 패치를 적어도 한 달에 한 번 적용하는지 지정합니다. 그렇지 않다면, 얼마나 자주 적용하나요? 패치 관리 방법에 대해 좀 더 자세히 설명해 주세요.	예. 이 프로세스를 격주로 수행하는 보안 팀이 있습니다.
	최종 사용자 디바이스 보안 7.2.2 - 자산 보안 - 엔드포인트 보안	엔드포인트 보안이 있나요?	엔드포인트 보안이 모든 디바이스에 설치되는지 지정합니다. 그렇다면, 도구와 유지 관리 방법에 대해	예. 보안 팀이 내부 도구를 사용하여 격주로 이 문제를 처리합니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
			자세히 설명해 주세요.	
	최종 사용자 디바이스 보안 7.2.3 - 자산 보안 - 자산 유지 관리 및 수리(수동 증명 필요)	승인을 받았으며 적절히 통제되는 도구를 사용하여 조직 자산을 유지 관리 및 수리하고 로깅하나요?	승인을 받았으며 적절히 통제되는 도구를 사용하여 자산을 유지 관리 및 수리하고 로깅하는지 지정합니다. 그렇다면, 관리 방법에 대해 좀 더 자세히 설명해 주세요.	예. 디바이스의 모든 유지 관리 작업이 로깅됩니다. 이 유지 관리 때문에 가동이 중지되지 않습니다.
	최종 사용자 디바이스 보안 7.2.4 - 자산 보안 - 디바이스 액세스 제어	디바이스에서 액세스 제어가 활성화되나요?	디바이스에서 액세스 제어(예: RBAC)가 활성화되는지 지정합니다.	예. 모든 디바이스에 대해 최소 권한 액세스가 구현됩니다.
디바이스 목록	최종 사용자 디바이스 보안 7.3.1 - 디바이스 로그 - 로그의 충분한 세부 정보(수동 증명 필요)	운영 체제 및 디바이스 로그에 인시던트 조사를 뒷받침할 수 있는 충분한 세부 정보가 로깅되나요?	인시던트 조사를 뒷받침할 수 있는 충분한 세부 정보(로그인 시도 성공 및 실패 횟수, 민감한 구성 설정 및 파일 변경 등)가 로그에 포함되는지 지정합니다. 그렇지 않으면, 인시던트 조사를 처리하는 방법에 대해 자세히 설명해 주세요.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	최종 사용자 디바이스 보안 7.3.2 - 디바이스 로그 - 디바이스 로그 액세스	디바이스 로그를 수정, 삭제 또는 부적절하게 액세스할 수 없도록 보호하나요?	디바이스 로그를 수정, 삭제 또는 부적절하게 액세스할 수 없도록 보호하는지 지정합니다. 그렇다면, 보호 이행 방법에 대해 자세히 설명해 주세요.	예. 로그 변경은 액세스 제어를 통해 이행됩니다. 로그를 변경할 때마다 알림이 제공됩니다.
	최종 사용자 디바이스 보안 7.3.3 - 디바이스 로그 - 로그 보존(수동 증명 필요)	공격을 조사하기에 충분한 시간 동안 로그가 보존되나요?	로그는 얼마나 오래 보존되나요?	예, 1년 동안 보존됩니다.
모바일 디바이스 관리	최종 사용자 디바이스 보안 7.4.1 - 모바일 디바이스 관리 - 모바일 디바이스 관리 프로그램	모바일 디바이스 관리 프로그램이 있나요?	모바일 디바이스 관리 프로그램이 있는지 지정합니다. 그렇다면, 모바일 디바이스 관리에 사용되는 도구를 지정하세요.	예. 내부 도구를 사용합니다.
	최종 사용자 디바이스 보안 7.4.2 - 모바일 디바이스 관리 - 프라이빗 모바일 디바이스에서 프로덕션 환경에 액세스(수동 증명 필요)	직원이 비관리형 프라이빗 모바일 디바이스를 사용하여 프로덕션 환경에 액세스하지 못하게 차단하나요?	직원이 비관리형 프라이빗 모바일 디바이스를 사용하여 프로덕션 환경에 액세스하지 못하게 차단하는지 지정합니다. 그렇지 않다면, 이 제어를 어떻게 적용하나요?	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	최종 사용자 디바이스 보안 7.4.3 - 모바일 디바이스 관리 - 모바일 디바이스에서 고객 데이터에 액세스(수동 증명 필요)	직원이 비관리형 프라이빗 모바일 디바이스를 사용하여 고객 데이터를 보거나 처리하지 못하게 차단하나요?	직원이 비관리형 모바일 디바이스를 사용하여 고객 데이터에 액세스하지 못하게 차단하는지 지정합니다. 그렇지 않다면, 액세스를 허용하는 사용 사례는 무엇인가요? 액세스를 어떻게 모니터링하나요?	예

인적 자원 컨트롤

인적 자원 컨트롤은 직원 채용, 급여 지급, 계약 종료 등의 프로세스 중에 민감한 데이터를 처리하는 직원 관련 부서를 평가합니다. 이 표에는 인적 자원 정책 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
인적 자원 정책	인적 자원 9.1.1 - 인적 자원 정책 - 직원의 신원 조회	고용 전에 신원을 조회하나요?	고용 전에 직원의 신원을 조회하는지 지정합니다.	예
	인적 자원 9.1.2 - 인적 자원 정책 - 직원 계약	고용 전에 고용 계약서에 서명하나요?	고용 전에 고용 계약서에 서명하는지 지정합니다.	예
	인적 자원 9.1.3 - 인적 자원 정책 - 직원 보안 교육	모든 직원이 정기적으로 보안 인식 교육을 받나요?	직원이 정기적으로 보안 교육을 받는지 지정합니다. 그렇다면, 얼	예. 직원은 매년 보안 교육을 받습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
			마나 자주 보안 교육을 받나요?	
	인적 자원 9.1.4 - 인적 자원 정책 - 정책 미준수에 대한 징계 절차	인적 자원 정책 미준수에 대한 징계 절차가 있나요?	인적 자원 정책 미준수에 대한 징계 절차가 있는지 지정합니다.	예
	인적 자원 9.1.5 - 인적 자원 정책 - 도급사/하도급사의 신원 조회(수동 증명 필요)	타사 공급업체, 도급사 및 하도급사의 신원을 조회하나요?	타사 공급업체, 도급사 및 하도급사의 신원을 조회하는지 지정합니다. 그렇다면, 신원 조회가 정기적으로 이루어지나요?	예. 신원 조회는 매년 실시됩니다.
	인적 자원 9.1.6 - 인적 자원 정책 - 계약 종료 시 자산 반환	계약 종료 시 자산 반환을 확인하는 절차가 있나요?	계약 종료 시 자산 반환을 확인하는 절차가 있는지 지정합니다.	예

인프라 보안 컨트롤

인프라 보안 컨트롤은 중요 자산을 위협과 취약성으로부터 보호합니다. 이 표에는 인프라 보안 정책 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
물리적 보안	인프라 보안 8.1.1 - 물리적 보안 - 시설에 대한 물리적 액세스	자산(예: 건물, 차량 또는 하드웨어)에 직접 액세스해야 하는 개인	자산(예: 건물, 차량 또는 하드웨어)에 직접 액세스해야 하는 개인	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
		은 신분증과 필요한 보안 인증 정보를 제시해야 하나요?	은 신분증과 필요한 보안 인증 정보를 제시해야 하는지 지정합니다.	
	인프라 보안 8.1.2 - 물리적 보안 - 준비된 물리적 보안 및 환경 제어 수단	데이터 센터와 사무실 건물에 물리적 보안 및 환경 제어 수단이 준비되어 있나요?	모든 시설에 물리적 보안 및 환경 제어 수단이 준비되어 있는지 지정합니다.	예
	인프라 보안 8.1.3 - 물리적 보안 - 방문자 액세스(수동 증명 필요)	방문자 액세스를 기록하나요?	방문자가 시설에 들어갈 수 있는 경우 방문자 액세스 로그를 유지하나요? 그렇다면, 로그를 얼마나 오래 유지하나요?	예. 로그는 1년 동안 보존됩니다.
네트워크 보안	인프라 보안 8.2.1 - 네트워크 보안 - 사용되지 않는 포트 및 서비스 비활성화(수동 증명 필요)	사용되지 않는 모든 포트와 서비스가 프로덕션 환경 및 시스템에서 비활성화되나요?	사용되지 않는 모든 포트와 서비스가 프로덕션 환경 및 시스템에서 비활성화되는지 지정합니다.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	인프라 보안 8.2.2 - 네트워크 보안 - 방화벽 사용	중요하고 민감한 시스템을, 덜 민감한 시스템을 사용하는 네트워크 세그먼트와 분리된 네트워크 세그먼트에 분리하기 위해 방화벽을 사용하나요?	중요하고 민감한 시스템을, 덜 민감한 시스템을 사용하는 네트워크 세그먼트와 분리된 네트워크 세그먼트에 분리하기 위해 방화벽을 사용하는지 지정합니다.	예
	인프라 보안 8.2.3 - 네트워크 보안 - 방화벽 규칙 검토	모든 방화벽 규칙을 정기적으로 검토하고 업데이트하나요?	방화벽 규칙을 얼마나 자주 검토하고 업데이트하나요?	예. 방화벽 규칙은 3개월마다 업데이트됩니다.
	인프라 보안 8.2.4 - 네트워크 보안 - 침입 탐지 및 방지 시스템	모든 민감한 네트워크 영역과 방화벽이 사용되는 곳에 침입 탐지 및 방지 시스템이 배포되어 있나요?	모든 민감한 네트워크 영역에서 침입 탐지 및 방지 시스템을 사용하는지 지정합니다.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	인프라 보안 8.2.5 - 네트워크 보안 - 보안 및 강화 표준	네트워크 디바이스에 대한 보안 및 강화 표준이 마련되어 있나요?	네트워크 디바이스에 대한 보안 및 강화 표준이 마련되어 있는지 지정합니다. 그렇다면, 이러한 표준을 구현하고 업데이트하는 빈도에 대한 세부 정보를 포함하여 좀 더 자세한 정보를 제공해 주세요.	예. 보안 및 강화 표준은 매월 네트워크 디바이스에 구현됩니다.
클라우드 서비스	인프라 보안 8.3.1 - 클라우드 서비스 - 애플리케이션을 호스팅하는 데 사용되는 플랫폼(수동 증명 필요)	애플리케이션을 호스팅하는 데 사용하는 클라우드 플랫폼을 나열합니다.	애플리케이션을 호스팅하는 데 사용하는 클라우드 플랫폼을 지정합니다.	AWS

위험 관리 및 인시던트 대응 컨트롤

위험 관리 및 인시던트 대응 컨트롤은 수용 가능한 것으로 간주되는 위험 수준과 위험 및 공격에 대응하기 위해 수행된 조치를 평가합니다. 이 표에는 위험 관리 및 인시던트 대응 정책 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
위험 평가	위험 관리 및 인시던트 대응 5.1.1 - 위험 평가	조직에 지장을 초래하는 인시던트 위험을 식별하고 해결하는 데 초	조직에 지장을 초래하는 인시던트 위험을 식별하고 해결하는 공식 프	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	- 위험 해결 및 식별	점을 맞춘 공식 프로세스가 있나요?	로세스가 있는지 지정합니다.	
	위험 관리 및 인시던트 대응 5.1.2 - 위험 평가 - 위험 관리 프로세스	평가 중에 식별된 위험의 처리를 관리하는 프로그램 또는 프로세스가 있나요?	위험 및 위험 완화를 관리하는 프로그램 또는 프로세스가 있는지 지정합니다. 그렇다면, 위험 관리 프로세스에 대해 좀 더 자세히 설명해 주세요.	예. 정기적으로 문제를 검토하고 수정하여 미준수 사항을 해결하고 있습니다. 다음은 환경에 영향을 미치는 모든 문제에서 확인되는 정보입니다. • 확인된 문제의 세부 정보 • 근본 원인 • 컨트롤 보정 • 심각도 • 소유자 • 단기 진로 • 장기 진로
	위험 관리 및 인시던트 대응 5.1.3 - 위험 평가 - 위험 평가	위험 평가를 자주 하나요?	위험 평가를 자주 하나요? 그렇다면, 위험 평가 빈도를 지정합니다.	예. 위험 평가는 6개월마다 이루어집니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	위험 관리 및 인시던트 대응 5.1.4 - 위험 평가 - 타사 공급업체 위험 평가	모든 타사 공급업체에 대한 위험 평가를 수행하나요?	모든 타사 공급업체에 대한 위험 평가를 수행하는지 지정합니다. 그렇다면, 얼마나 자주 하나요?	이 샘플에는 해당하지 않습니다.
	위험 관리 및 인시던트 대응 5.1.5 - 위험 평가 - 계약 변경 시 위험 재평가	서비스 제공 또는 계약 변경이 발생할 때 위험 평가를 수행하나요?	서비스 제공 또는 계약 변경이 발생할 때마다 위험 평가를 수행하는지 지정합니다.	이 샘플에는 해당하지 않습니다.
	위험 관리 및 인시던트 대응 5.1.6 - 위험 평가 - 위험 수용(수동 증명 필요)	경영진이 사정을 다 알고 객관적으로 위험을 수용하고 실행 계획을 승인하는 프로세스가 있나요?	경영진이 위험을 이해 및 수용하고, 위험 관련 문제를 해결하기 위한 실행 계획과 일정을 승인하는 프로세스가 있는지 지정합니다. 각 위험의 이면에 숨어 있는 지표에 대한 세부 정보를 경영진에게 제공하는 것도 이 프로세스에 포함되어 있나요?	예. 경영진이 위험을 승인하기 전에, 위험 심각도 및 적절히 완화하지 않으면 발생할 수 있는 잠재적 문제에 대한 세부 정보가 경영진에게 제공됩니다.
	위험 관리 및 인시던트 대응 5.1.7 - 위험 평가 - 위험 지표(수동 증명 필요)	위험 지표를 정의, 모니터링 및 보고하는 조치가 마련되어 있나요?	위험 지표를 정의, 모니터링 및 보고하는 프로세스가 있는지 지정합니다.	예

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
인시던트 관리	위험 관리 및 인시던트 대응 5.2.1 - 인시던트 관리 - 인시던트 대응 계획	공식적인 인시던트 대응 계획이 있나요?	공식적인 인시던트 대응 계획이 있는지 지정합니다.	예
	위험 관리/인시던트 대응 5.2.2 - 인시던트 관리 - 보안 인시던트 신고 연락처(수동 증명 필요)	고객이 보안 인시던트를 신고할 수 있는 프로세스가 있나요?	고객이 보안 인시던트를 신고하는 프로세스가 있는지 지정합니다. 그렇다면, 고객이 보안 인시던트를 신고하려면 어떻게 해야 하나요?	예. 고객은 example.com에 인시던트를 신고할 수 있습니다.
	위험 관리 및 인시던트 대응 5.2.3 - 인시던트 관리 - 인시던트 및 주요 활동 보고	주요 활동을 보고하나요?	주요 활동을 보고하나요? 주요 활동 보고에 대한 SLA는 무엇인가요?	예. 모든 주요 활동은 일주일 내에 보고됩니다.
	위험 관리 및 인시던트 대응 5.2.4 - 인시던트 관리 - 인시던트 복구	재해 복구 계획이 있나요?	인시던트 발생 후 복구 계획이 있는지 지정합니다. 그렇다면, 복구 계획에 대해 자세히 설명해 주세요.	예. 인시던트 발생 후 24시간 내에 복구가 완료됩니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	위험 관리 및 인시던트 대응 5.2.5 - 인시던트 관리 - 공격 발생 시 구매자가 사용할 수 있는 로그(수동 증명 필요)	공격 발생 시 고객이 관련 리소스(예: 로그, 인시던트 보고서 또는 데이터)를 사용할 수 있나요?	공격 또는 인시던트 발생 시 고객이 공격 또는 인시던트와 관련된 리소스(예: 로그, 인시던트 보고서 또는 데이터)를 사용할 수 있나요?	예
	위험 관리 및 인시던트 대응 5.2.6 - 인시던트 관리 - 보안 게시판(수동 증명 필요)	애플리케이션에 영향을 미치는 최신 공격 및 취약성에 대해 설명하는 보안 게시판이 있나요?	애플리케이션에 영향을 미치는 최신 공격 및 취약성에 대해 설명하는 보안 게시판이 있는지 지정합니다. 그렇다면, 자세한 정보를 제공해 주세요.	예. 고객은 example.com에 인시던트를 신고할 수 있습니다.
인시던트 탐지	위험 관리 및 인시던트 대응 5.3.1 - 인시던트 탐지 - 종합 로깅	인시던트의 식별 및 완화를 지원하는 포괄적인 로깅이 있나요?	포괄적인 로깅이 사용되는지 지정합니다. 시스템에서 로깅할 수 있는 이벤트 유형을 확인합니다. 로그는 얼마나 오래 보존되나요?	예. 애플리케이션, 디바이스, AWS 서비스(예: AWS CloudTrail, AWS Config), VPC 흐름 로그와 같은 이벤트가 로깅됩니다. 로그는 1년 동안 보존됩니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
	위험 관리 및 인시던트 대응 5.3.2 - 인시던트 탐지 - 로그 모니터링	로그 모니터링과 같은 탐지 메커니즘을 사용하여 비정상적이거나 의심스러운 활동을 모니터링하고 경고를 보내나요?	정기적으로 보안 모니터링 및 경고를 수행하는지 지정합니다. 그렇다면, 비정상적이거나 의심스러운 행동에 대한 로그 모니터링이 포함되나요?	예. 모든 로그를 모니터링하여 여러 번의 로그인 실패, 일반적이지 않은 지리적 위치에서의 로그인, 기타 의심스러운 경고와 같은 비정상적인 동작을 탐지합니다.
	위험 관리 및 인시던트 대응 5.3.3 - 인시던트 탐지 - 타사 데이터 침해	하도급사의 보안, 개인 정보 보호 또는 데이터 침해 문제를 식별, 탐지, 기록하는 프로세스가 있나요?	타사 공급업체 또는 하도급사의 데이터 침해, 보안 문제 또는 개인 정보 보호 문제를 식별하고 탐지하는 프로세스가 마련되어 있는지 지정합니다.	예
인시던트 알림에 대한 SLA	위험 관리 및 인시던트 대응 5.4.1 - 인시던트 알림에 대한 SLA(수동 증명 필요)	인시던트 또는 위반에 대한 알림 전송과 관련된 SLA는 무엇인가요?	인시던트 또는 위반에 대한 알림 전송과 관련된 SLA는 무엇인가요?	7일

보안 및 구성 정책 컨트롤

보안 및 구성 정책 컨트롤은 조직의 자산을 보호하는 보안 정책 및 보안 구성을 평가합니다. 이 표에는 보안 및 구성 정책 컨트롤의 값과 해당 설명이 나열되어 있습니다.

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
정보 보안 정책	보안 및 구성 정책 10.1.1 - 정보 보안 정책 - 정보 보안 정책	보안 팀이 소유하고 관리하는 정보 보안 정책이 있나요?	정보 보안 정책이 있는지 지정합니다. 그렇다면, 수동 증거를 공유하거나 업로드하세요.	예. 우리는 NIST 프레임워크를 기반으로 보안 정책을 수립합니다.
	보안 및 구성 정책 10.1.2 - 정보 보안 정책 - 정책 검토	모든 보안 정책을 매년 검토하나요?	보안 정책을 매년 검토하는지 지정합니다. 그렇지 않다면, 정책을 얼마나 자주 검토하나요?	예. 매년 검토합니다.
보안 구성 정책	보안 및 구성 정책 10.2.1 - 보안 구성 정책 - 보안 구성(수동 증명 필요)	보안 구성 표준을 유지 관리 및 문서화하고 있나요?	모든 보안 구성 표준을 유지 관리 및 문서화하고 있는지 지정합니다. 그렇다면, 수동 증거를 공유하거나 업로드하세요.	예
	보안 및 구성 정책 10.2.2 - 보안 구성 정책 - 보안 구성 검토(수동 증명 필요)	보안 구성을 1년에 한 번 이상 검토하나요?	보안 구성을 1년에 한 번 이상 검토하는지 지정합니다. 그렇지 않다면, 검토 빈도를 지정하세요.	예. 3개월마다 검토합니다.
	보안 및 구성 정책 10.2.3 - 보안 구성 정책 - 구성 변경	구성 변경 사항이 로깅되나요?	구성 변경 사항이 로깅되는지 지정합니다. 그렇다면, 로그를 얼마	예. 모든 구성 변경 사항이 모니터링되고 로깅됩니다. 구성이 변경되면 경고가 발생

컨트롤 세트	컨트롤 제목	컨트롤 설명	증거 추출 세부 정보	샘플 값
			나 오래 유지하나요?	합니다. 로그는 6개월 동안 보존됩니다.

AWS Marketplace Vendor Insights를 사용하여 구매자로 스냅샷 내보내기

스냅샷은 보안 프로필의 특정 시점 태세입니다. 스냅샷을 내보내면 데이터를 오프라인으로 다운로드 및 검토하고, 증거 데이터를 검토하고, 제품을 비교할 수 있습니다.

스냅샷 내보내기

JSON 또는 CSV 형식으로 내보낼 수 있습니다. 스냅샷을 내보내려면 다음 단계를 수행합니다.

1. AWS Management Console에 로그인한 다음 AWS Marketplace 콘솔을 엽니다.
2. Vendor Insights를 선택합니다.
3. Vendor Insights에서 제품을 선택합니다.
4. 보안 및 규정 준수 탭에서 요약 섹션으로 이동하여 내보내기를 선택합니다.
5. 드롭다운 목록에서 다운로드(JSON) 또는 다운로드(CSV)를 선택합니다.

AWS Marketplace Vendor Insights의 액세스 권한 제어

AWS Identity and Access Management(IAM)는 AWS 리소스에 대한 액세스를 쉽게 제어할 수 있는 AWS 서비스입니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다. 관리자는 AWS Marketplace 리소스를 사용할 수 있는 인증(로그인) 및 권한 부여(권한 있음)를 받을 수 있는 사람을 제어합니다. AWS Marketplace Vendor Insights는 IAM을 사용하여 판매자 데이터, 평가, 판매자 자체 증명 및 산업 표준 감사 보고서에 대한 액세스 권한을 제어합니다.

AWS Marketplace Management Portal에서 누가 무엇을 할 수 있는지 제어하는 좋은 방법은 IAM를 사용하여 사용자와 그룹을 생성하는 것입니다. 그런 다음 사용자를 그룹에 추가하고 그룹을 관리합니다. 읽기 전용 권한을 제공하는 정책 또는 권한을 해당 그룹에 할당할 수 있습니다. 읽기 전용 액세스가 필

요한 다른 사용자들이 있는 경우에는 이들의 AWS 계정에 권한을 추가하지 말고 생성한 그룹에 이들을 추가하면 됩니다.

정책은 사용자, 그룹 또는 역할에 적용되는 권한을 정의하는 문서입니다. 권한은 사용자가 AWS에서 수행할 수 있는 작업을 결정합니다. 정책은 일반적으로 특정 작업에 대한 액세스를 허용하며 Amazon EC2 인스턴스, Amazon S3 buckets 버킷과 같은 특정 리소스에 대한 작업을 허용하도록 선택적으로 권한을 부여할 수 있습니다. 정책은 액세스를 명시적으로 거부할 수도 있습니다. 권한은 특정 리소스에 대한 액세스를 허용하거나 거부하는 정책 내 문입니다.

> **Important**
>
> 생성하는 모든 사용자는 자신의 자격 증명을 사용하여 인증합니다. 그러나 이들은 동일한 AWS 계정을 사용합니다. 사용자에 의한 모든 변경은 전체 계정에 영향을 줄 수 있습니다.

AWS Marketplace은 이러한 권한이 있는 사람이 AWS Marketplace Management Portal에서 취할 수 있는 조치를 제어하도록 정의된 권한이 있습니다. AWS Marketplace가 여러 권한을 결합하여 생성하고 관리하는 정책도 있습니다. 이 `AWSMarketplaceSellerProductsFullAccess` 정책은 사용자에게 AWS Marketplace Management Portal의 제품에 대한 전체 액세스 권한을 부여합니다.

사용 가능한 작업, 리소스 및 조건 키에 대한 자세한 내용은 서비스 승인 참조의 AWS Marketplace Vender Insights에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

AWS Marketplace Vendor Insights 구매자의 권한

구매자는 AWS Marketplace Vendor Insights에 대한 IAM 정책에서 다음 권한을 사용할 수 있습니다. 이러한 권한을 단일 IAM 정책에 결합하여 원하는 권한을 부여할 수 있습니다.

`GetProfileAccessTerms`

`GetProfileAccessTerms`는 사용자가 AWS Marketplace Vendor Insights 프로필을 검토, 수락 및 액세스하는 데 필요한 조건을 검색할 수 있도록 허용합니다.

작업 그룹: 읽기 전용 및 읽기-쓰기.

필수 리소스: `SecurityProfile`.

`ListEntitledSecurityProfiles`

`ListEntitledSecurityProfiles`는 사용자가 활성 읽기 권한이 있는 보안 프로필을 모두 나열할 수 있도록 허용합니다.

작업 그룹: 읽기 전용, 나열 전용 및 읽기-쓰기.

필수 리소스: 없음

ListEntitledSecurityProfileSnapshots

ListEntitledSecurityProfileSnapshots는 사용자가 SecurityProfile을 읽을 수 있는 활성 읽기 권한이 있는 보안 프로필의 보안 프로필 스냅샷을 나열할 수 있도록 허용합니다.

작업 그룹: 읽기 전용, 나열 전용 및 읽기-쓰기.

필수 리소스: SecurityProfile

GetEntitledSecurityProfileSnapshot

GetEntitledSecurityProfileSnapshot은 사용자가 활성 읽기 권한이 있는 보안 프로필의 보안 프로필 스냅샷 세부 정보를 가져올 수 있도록 허용합니다.

작업 그룹: 읽기 전용 및 읽기-쓰기.

필수 리소스: SecurityProfile

AWS Marketplace 보안

당사는 우수 판매자의 소프트웨어를 나열하고, 엄선된 제품의 품질을 유지하기 위해 적극적으로 노력하고 있습니다. 고객마다 처한 상황이 다르기 때문에 고객이 올바른 구매 결정을 내릴 수 있도록 AWS Marketplace에 나열된 제품에 대한 정보를 충분히 제공하는 것이 당사의 목적입니다.

> **Note**
>
> AWS Data Exchange의 데이터 제품 보안에 대한 자세한 내용은 AWS Data Exchange 사용 설명서의 보안을 참조하세요.
> AWS Marketplace의 판매자 보안에 대한 자세한 내용은 AWS Marketplace 판매자 설명서의 AWS Marketplace 보안을 참조하세요.

판매자와 공유되는 구독자 정보

다음과 같은 이유로 연락처 정보를 판매자와 공유할 수 있습니다.

- 고객 교육 및 기술 지원을 제공해야 하는 경우.
- 소프트웨어 활성화, 구성 및 콘텐츠 사용자 지정.
- 내부적으로 영업 팀 보상.

또한 판매자가 자사 영업 팀을 보완할 수 있도록 회사 이름, 전체 주소 및 사용 요금 같은 정보를 판매자와 공유할 수 있습니다. 그 밖에 마케팅 캠페인의 효과를 평가하는 데 도움이 될 수 있는 특정 정보 역시 판매자와 공유할 수 있습니다. 판매자는 이미 보유하고 있는 정보와 함께 이러한 정보를 사용하여 영업 팀에 대한 보수나 특정 구매자의 사용량을 확인할 수 있습니다.

그 외에는 사용자가 정보를 공유할 수 있는 권한을 부여했거나 법률 혹은 법률 또는 규정을 준수할 목적으로 판매자에게 정보를 제공해야 하는 경우가 아니라면 일반적으로 판매자와 고객 정보를 공유하지 않으며, 개인 식별이 불가능한 정보만 공유합니다.

IAM 정책을 IPv6로 업그레이드

AWS Marketplace 고객은 IAM 정책을 사용하여 허용되는 IP 주소 범위를 설정하고, 구성된 범위를 벗어나는 IP 주소가 AWS Marketplace 리소스에 액세스하지 못하게 차단합니다.

AWS Marketplace 웹 사이트 도메인이 IPv6 프로토콜로 업그레이드됩니다.

IP 주소 필터링 정책이 IPv6 주소를 처리하도록 업데이트되지 않으면 클라이언트가 AWS Marketplace 웹 사이트의 리소스에 대한 액세스 권한을 잃을 수 있습니다.

IPv4에서 IPv6로 업그레이드 시 영향을 받는 고객

이중 주소 지정을 사용하는 고객은 이번 업그레이드의 영향을 받습니다. 이중 주소 지정이란 네트워크에서 IPv4와 IPv6를 모두 지원한다는 의미입니다.

이중 주소 지정을 사용하는 경우 현재 IPv4 형식 주소로 구성된 IAM 정책을 업데이트하여 IPv6 형식 주소를 포함해야 합니다.

액세스 문제에 대한 도움이 필요하면 AWS Support에 문의하세요.

> **Note**
>
> 다음 고객은 이번 업그레이드의 영향을 받지 않습니다.
>
> - IPv4 네트워크만 사용하는 고객.
> - IPv6 네트워크만 사용하는 고객.

IPv6란?

IPv6는 결국에는 IPv4를 대체하기 위해 개발된 차세대 IP 표준입니다. 이전 버전인 IPv4는 32비트 주소 지정 체계를 사용하여 43억 개의 디바이스를 지원합니다. IPv6는 128비트 주소 지정 체계를 사용하여 약 340조(또는 2의 128승) 개의 디바이스를 지원합니다.

```
2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

IPv6에 대한 IAM 정책 업데이트

IAM 정책은 현재 `aws:SourceIp` 필터를 사용하여 허용되는 IP 주소 범위를 설정하는 데 사용됩니다.

이중 주소 지정은 IPv4 트래픽과 IPV6 트래픽을 모두 지원합니다. 네트워크에서 이중 주소 지정을 사용하는 경우 IP 주소 필터링에 사용되는 IAM 정책이 IPv6 주소 범위를 포함하도록 업데이트해야 합니다.

예를 들어 이 Amazon S3 버킷 정책은 허용되는 IPv4 주소 범위 `192.0.2.0.*` 및 `203.0.113.0.*`을 `Condition` 요소에서 식별합니다.

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*",
                    "*203.0.113.0/24*"
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
    }
}
```

이 정책을 업데이트하려면 정책의 Condition 요소가 IPv6 주소 범위 2001:DB8:1234:5678::/64 및 2001:cdba:3257:8593::/64를 포함하도록 업데이트해야 합니다.

> **Note**
>
> 기존 IPv4 주소는 이전 버전과의 호환성에 필요하므로 제거하지 마세요.

```
"Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*", <<DO NOT remove existing IPv4 address>>
                    "*203.0.113.0/24*", <<DO NOT remove existing IPv4 address>>
                    "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
                    "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
```

```
        }
```

IAM을 사용한 액세스 권한 관리에 대한 자세한 내용은 AWS Identity and Access Management IAM 사용 설명서의 관리형 정책과 인라인 정책을 참조하세요.

IPv4에서 IPv6로 업데이트 후 네트워크 테스트

IAM 정책을 IPv6 형식으로 업데이트한 후에는 네트워크가 IPv6 엔드포인트에 액세스하는지 여부와 AWS Marketplace 웹 사이트 기능을 테스트할 수 있습니다.

주제

- Linux/Unix 또는 Mac OS X를 사용하여 네트워크 테스트
- Windows 7 또는 Windows 10에서 네트워크 테스트
- AWS Marketplace 웹 사이트 테스트

Linux/Unix 또는 Mac OS X를 사용하여 네트워크 테스트

Linux/Unix 또는 Mac OS X를 사용하는 경우 다음 curl 명령을 사용하여 네트워크가 IPv6 엔드포인트에 액세스하는지 테스트할 수 있습니다.

```
curl -v -s -o /dev/null http://ipv6.ec2-reachability.amazonaws.com/
```

예를 들어 IPv6을 통해 연결된 경우 연결된 IP 주소가 다음 정보를 표시합니다.

```
* About to connect() to aws.amazon.com port 443 (#0)
*   Trying IPv6 address... connected
* Connected to aws.amazon.com (IPv6 address) port 443 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1 OpenSSL/1.0.1t
 zlib/1.2.3
> Host: aws.amazon.com
```

Windows 7 또는 Windows 10에서 네트워크 테스트

Windows 7 또는 Windows 10을 사용하는 경우 네트워크가 IPv6 또는 IPv4를 통해 듀얼 스택 엔드포인트에 액세스할 수 있는지 테스트할 수 있습니다. 다음 예와 같이 ping 명령을 사용합니다.

```
ping aws.amazon.com
```

IPv6를 통해 엔드포인트에 액세스하는 경우 이 명령은 IPv6 주소를 반환합니다.

AWS Marketplace 웹 사이트 테스트

업데이트 후 AWS Marketplace 웹 사이트 기능을 테스트하는 방법은 주로 정책 작성 방식과 정책의 용도에 따라 달라집니다. 일반적으로 정책에 지정된 기능이 의도한 대로 작동하는지 확인해야 합니다.

다음 시나리오는 AWS Marketplace 웹 사이트 기능 테스트를 시작하는 데 도움이 될 수 있습니다.

AWS Marketplace 웹 사이트에서 구매자로서 다음 작업을 수행할 수 있는지 테스트합니다.

- AWS Marketplace 제품을 구독합니다.
- AWS Marketplace 제품을 구성합니다.
- AWS Marketplace 제품을 시작하거나 이행합니다.

AWS Marketplace 웹 사이트에서 판매자로서 다음 작업을 수행할 수 있는지 테스트합니다.

- 기존 AWS Marketplace 제품을 관리합니다.
- 새 AWS Marketplace 제품을 생성합니다.

AWS Marketplace 구독에 대한 액세스 제어

AWS IAM Identity Center을 사용하면 직원 자격 증명을 안전하게 생성 또는 연결하고 AWS 계정 및 애플리케이션 전체의 직원 액세스 권한을 중앙에서 관리할 수 있습니다. IAM Identity Center는 조직의 규모와 유형에 관계없이 AWS에서 인력 인증 및 권한 부여에 사용하면 좋은 접근 방식입니다. 추가 구성 지침은 AWS 보안 참조 아키텍처를 참조하세요.

IAM Identity Center는 사용자가 자신에게 할당된 AWS 계정, 역할, 클라우드 애플리케이션 및 사용자 지정 애플리케이션을 한 곳에서 찾고 액세스할 수 있는 사용자 포털을 제공합니다. IAM Identity Center는 연결된 디렉터리의 사용자 및 그룹에 Single Sign-On 액세스 권한을 할당하고 권한 세트를 사용하여 사용자 및 그룹의 액세스 수준을 결정합니다. 이렇게 하면 임시 보안 자격 증명을 사용할 수 있습니다. AWS Marketplace에 액세스할 수 있는 특정 AWS 관리형 역할을 할당하여 액세스 수준을 정의하는 방식으로 AWS 조직 전체의 AWS Marketplace 구독 관리를 위임할 수 있습니다.

예를 들어 고객 A는 페더레이션을 통해 역할을 맡으며 해당 역할에는 `ManagedMarketplace_ViewOnly` 정책이 연결되었습니다. 따라서 고객 A는 AWS Marketplace에서만 구독을 볼 수 있습니다. 구독을 볼 권한이 있는 IAM 역할을 생성하고 고객 A에게 이 역할을 수임할 수 있는 권한을 부여할 수 있습니다.

AWS Marketplace에 액세스할 수 있는 IAM 역할 생성

IAM 역할을 사용해 AWS 리소스에 대한 액세스 권한을 위임할 수 있습니다.

AWS Marketplace 권한 할당을 위한 그룹을 생성하는 방법

1. IAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 [역할(Roles)]을 선택한 다음, [역할 생성(Create role)]을 선택합니다.
3. AWS 계정를 선택합니다.
4. 권한 추가에서 다음 정책 중 하나를 선택합니다.
   - 구독을 볼 수만 있고 변경할 수 없는 권한을 허용하려면 AWSMarketplaceRead-only를 선택합니다.
   - 구독 및 구독 취소 권한을 허용하려면 AWSMarketplaceManageSubscriptions를 선택합니다.
   - 구독을 완전히 제어할 수 있도록 허용하려면 AWSMarketplaceFullAccess를 선택합니다.
5. 다음(Next)을 선택합니다.
6. 역할 이름에 역할의 이름을 입력합니다. 예를 들어 *MarketplaceReadOnly* 또는 *MarketplaceFullAccess*를 입력합니다. 그런 다음 역할 생성(Create role)을 선택합니다. 자세한 내용은 IAM 역할 생성을 참조하세요.

> **Note**
>
> 지정된 계정의 관리자는 해당 계정의 사용자에게 이 역할을 맡을 수 있는 권한을 부여할 수 있습니다.

각 사용자 페르소나가 사용자 지정 권한이 있는 IAM 역할을 사용할 수 있도록 이전 단계를 반복하여 권한 세트가 다른 역할을 더 많이 생성합니다.

여기에 설명된 AWS 관리형 정책의 권한으로 제한되지 않습니다. IAM을 이용하여 사용자 지정 권한이 있는 정책을 생성한 다음, 해당 정책을 IAM 역할에 추가할 수 있습니다. 자세한 내용은 IAM 정책 관리 및 IAM 자격 증명 권한 추가를 참조하세요.

AWS Marketplace의 AWS 관리형 정책

AWS 관리형 정책을 사용하여 기본 AWS Marketplace 권한을 제공할 수 있습니다. 그런 다음, 고유 시나리오의 경우 자체 정책을 생성하여 시나리오에 대한 특정 요구 사항이 있는 역할에 적용할 수 있습니다. 권한이 있는 사용자를 제어할 수 있는 기본 AWS Marketplace 관리형 정책은 다음과 같습니다.

- `AWSMarketplaceRead-only`
- `AWSMarketplaceManageSubscriptions`
- `AWSPrivateMarketplaceRequests`
- `AWSPrivateMarketplaceAdminFullAccess`
- `AWSMarketplaceFullAccess`

또한 AWS Marketplace는 특정 시나리오를 위한 특수 관리형 정책을 제공합니다. AWS Marketplace 구매자를 위한 AWS 관리형 정책의 전체 목록과 이러한 정책이 제공하는 권한에 대한 설명은 AWS Marketplace 구매자에 대한 AWS 관리형 정책 섹션을 참조하세요.

License Manager 사용 권한

AWS Marketplace는 AWS License Manager와 통합되므로 구독하는 제품의 라이선스를 관리하고 조직의 계정 간에 공유할 수 있습니다. AWS Marketplace에서 구독의 전체 세부 정보를 보려면 사용자가 AWS License Manager에서 라이선스 정보를 나열할 수 있어야 합니다.

사용자에게 AWS Marketplace 제품 및 구독에 대한 모든 데이터를 볼 수 있는 권한을 부여하려면 다음 권한을 추가합니다.

- `license-manager:ListReceivedLicenses`

권한 설정에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 관리를 참조하세요.

추가 리소스

IAM 역할 관리에 대한 자세한 내용은 IAM 사용 설명서의 IAM 자격 증명(사용자, 사용자 그룹 및 역할)을 참조하세요.

IAM 권한 및 정책 관리에 대한 자세한 내용은 IAM 사용 설명서의 정책을 사용한 AWS 리소스 액세스 제어를 참조하세요.

AWS Data Exchange 데이터 제품의 IAM 권한 및 정책 관리에 대한 자세한 내용은 AWS Data Exchange 사용 설명서의 AWS Data Exchange의 자격 증명 및 액세스 관리를 참조하세요.

AWS Marketplace 구매자에 대한 AWS 관리형 정책

AWS 관리형 정책은 AWS에 의해 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있기 때문에 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

이 섹션에는 AWS Marketplace에 대한 구매자 액세스를 관리하는 데 사용되는 각 정책이 나열됩니다. 판매자 정책에 대한 자세한 내용은 AWS Marketplace 판매자 설명서의 AWS Marketplace 판매자에 대한 AWS 관리형 정책을 참조하세요.

주제

- AWS 관리형 정책: AWSMarketplaceDeploymentServiceRolePolicy
- AWS 관리형 정책: AWSMarketplaceFullAccess
- AWS관리형 정책: AWSMarketplaceImageBuildFullAccess
- AWS관리형 정책: AWSMarketplaceLicenseManagementServiceRolePolicy
- AWS관리형 정책: AWSMarketplaceManageSubscriptions
- AWS관리형 정책: AWSMarketplaceProcurementSystemAdminFullAccess
- AWS관리형 정책: AWSMarketplaceRead 전용
- AWS관리형 정책: AWSPrivateMarketplaceAdminFullAccess
- AWS관리형 정책: AWSPrivateMarketplaceRequests
- AWS 관리형 정책: AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWS 관리형 정책: AWSVendorInsightsAssessorFullAccess

- AWS 관리형 정책: AWSVendorInsightsAssessorReadOnly
- AWS 관리형 정책으로 AWS Marketplace 업데이트

AWS 관리형 정책: AWSMarketplaceDeploymentServiceRolePolicy

AWSMarketplaceDeploymentServiceRolePolicy를 IAM 엔터티에 연결할 수 없습니다. 이 정책은 AWS Marketplace에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 설명은 AWS Marketplace에 서비스 연결 역할 사용 섹션을 참조하세요.

이 정책은 AWS Marketplace에서 사용자 대신 AWS Secrets Manager에 보안 정보로 저장되는 배포 관련 파라미터를 관리할 수 있는 권한을 기여자에게 부여합니다.

AWS 관리형 정책: AWSMarketplaceFullAccess

AWSMarketplaceFullAccess 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 AWS Marketplace 및 관련 서비스에 구매자 및 판매자로 액세스할 수 있는 전체 액세스 권한을 허용하는 관리 권한을 부여합니다. 이러한 권한으로 AWS Marketplace 소프트웨어를 구독 및 구독 해지하고, AWS Marketplace에서 AWS Marketplace 소프트웨어 인스턴스를 관리하고, 계정에서 프라이빗 마켓플레이스를 생성 및 관리하고, Amazon EC2, AWS CloudFormation 및 Amazon EC2 Systems Manager에 액세스할 수 있습니다.

권한 세부 정보

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:*",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStackResource",
                "cloudformation:DescribeStackResources",
                "cloudformation:DescribeStacks",
                "cloudformation:List*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:DescribeAccountAttributes",
```

```
                "ec2:DescribeAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:DeregisterImage",
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:CreateImage",
                "ec2:DescribeInstanceStatus",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "sns:ListTopics",
                "sns:GetTopicAttributes",
                "sns:CreateTopic",
                "iam:GetRole",
                "iam:GetInstanceProfile",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
```

```
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::*image-build*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish",
                "sns:setTopicAttributes"
            ],
            "Resource": "arn:aws:sns:*:*:*image-build*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ec2.amazonaws.com"
                    ]
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ],
                    "iam:AssociatedResourceARN": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
                    ]
                }
            }
        }
    ]
}
```

AWS관리형 정책: AWSMarketplaceImageBuildFullAccess

> **Important**
>
> AWS Marketplace는 2024년 4월에 프라이빗 이미지 빌드 제공 방법을 중단할 예정입니다. 제공 방법은 중단되기 전까지는 기존 구독자만 사용할 수 있습니다. 자세한 내용은 프라이빗 이미지 빌드를 참조하세요.

`AWSMarketplaceImageBuildFullAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 기여자에게 AWS Marketplace 프라이빗 이미지 빌드 기능에 대한 전체 액세스 권한을 부여합니다. 프라이빗 이미지 생성 권한 외에도 이미지에 태그를 추가하고 Amazon EC2 인스턴스를 시작 및 종료할 수 있는 권한을 제공합니다.

권한 세부 정보

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListBuilds",
                "aws-marketplace:StartBuild",
                "aws-marketplace:DescribeBuilds"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/marketplace-image-build:build-id": "*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/*Automation*",
                "arn:aws:iam::*:role/*Instance*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "ec2.amazonaws.com"
                    ]
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "ec2:DeregisterImage",
                "ec2:CopyImage",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DeleteSnapshot",
                "ec2:CreateImage",
                "ec2:RunInstances",
                "ec2:DescribeInstanceStatus",
                "sns:GetTopicAttributes",
                "iam:GetRole",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::*image-build*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*::image/*",
                "arn:aws:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish"
            ],
            "Resource": [
                "arn:aws:sns:*:*:*image-build*"
            ]
        }
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ],
                    "iam:AssociatedResourceARN": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
```

```
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
                    ]
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/marketplace-image-build:build-id": "*"
                },
                "StringNotEquals": {
                    "ec2:CreateAction": "RunInstances"
                }
            }
        }
    ]
}
```

AWS관리형 정책: AWSMarketplaceLicenseManagementServiceRolePolicy

IAM AWSMarketplaceLicenseManagementServiceRolePolicy 엔티티에 연결할 수 없습니다. 이 정책은 AWS Marketplace이(가) 사용자를 대신하여 작업을 수행할 수 있도록 서비스 링크 역할에 연결됩니다. 자세한 설명은 AWS Marketplace에 서비스 연결 역할 사용 섹션을 참조하세요.

이 정책은 AWS Marketplace가 구매자 대신 라이선스를 관리할 수 있도록 허용하는 권한을 기여자에게 부여합니다.

권한 세부 정보

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

```
                "organizations:DescribeOrganization",
                "license-manager:ListReceivedGrants",
                "license-manager:ListDistributedGrants",
                "license-manager:GetGrant",
                "license-manager:CreateGrant",
                "license-manager:CreateGrantVersion",
                "license-manager:DeleteGrant",
                "license-manager:AcceptGrant"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS관리형 정책: AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 기여자에게 AWS Marketplace 제품을 구독 및 구독 해지할 수 있는 권한을 부여합니다.

권한 세부 정보

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-marketplace:ViewSubscriptions",
                "aws-marketplace:Subscribe",
                "aws-marketplace:Unsubscribe"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateListings"
            ]
        }
    ]
}
```

AWS관리형 정책: AWSMarketplaceProcurementSystemAdminFullAccess

`AWSMarketplaceProcurementSystemAdminFullAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 조직의 계정을 나열하는 권한을 포함하여 AWS Marketplace eProcurement 통합의 모든 측면을 관리할 수 있는 권한을 관리자에게 부여합니다. eProcurement 통합에 대한 자세한 내용은 조달 시스템과 AWS Marketplace 통합 섹션을 참조하세요.

권한 세부 정보

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:PutProcurementSystemConfiguration",
                "aws-marketplace:DescribeProcurementSystemConfiguration",
                "organizations:Describe*",
                "organizations:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS관리형 정책: AWSMarketplaceRead 전용

AWSMarketplaceRead-only 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 AWS Marketplace에서 계정의 제품, 비공개 제안 및 구독을 볼 수 있고 계정의 Amazon EC2, AWS Identity and Access Management 및 Amazon SNS 리소스를 볼 수 있는 읽기 전용 권한을 부여합니다.

권한 세부 정보

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Action": [
                "aws-marketplace:ViewSubscriptions",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListBuilds",
                "aws-marketplace:DescribeBuilds",
                "iam:ListRoles",
                "iam:ListInstanceProfiles",
                "sns:GetTopicAttributes",
                "sns:ListTopics"
            ]
        },
        {
            "Resource": "*",
            "Effect": "Allow",
```

```
            "Action": [
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ]
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateListings"
            ]
        }
    ]
}
```

AWS관리형 정책: AWSPrivateMarketplaceAdminFullAccess

`AWSPrivateMarketplaceAdminFullAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 관리자에게 계정(또는 조직)의 프라이빗 마켓플레이스를 관리할 수 있는 전체 액세스 권한을 부여합니다. 여러 관리자 사용에 대한 자세한 내용은 the section called “프라이빗 마켓플레이스 관리자를 위한 사용자 지정 정책 생성” 섹션을 참조하세요.

권한 세부 정보

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrivateMarketplaceRequestPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceCatalogAPIPermissions",
```

```
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:StartChangeSet",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceCatalogTaggingPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:TagResource",
                "aws-marketplace:UntagResource",
                "aws-marketplace:ListTagsForResource"
            ],
            "Resource": "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
        },
        {
            "Sid": "PrivateMarketplaceOrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS관리형 정책: AWSPrivateMarketplaceRequests

AWSPrivateMarketplaceRequests 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 프라이빗 마켓플레이스에 제품을 추가하도록 요청하고 해당 요청을 볼 수 있는 권한을 기여자에게 부여합니다. 이러한 요청은 프라이빗 마켓플레이스 관리자가 승인하거나 거부해야 합니다.

권한 세부 정보

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSServiceRoleForPrivateMarketplaceAdminPolicy

AWSServiceRoleForPrivateMarketplaceAdminPolicy를 IAM 엔터티에 연결할 수 없습니다. 이 정책은 AWS Marketplace에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 설명은 AWS Marketplace에 서비스 연결 역할 사용 섹션을 참조하세요.

이 정책은 기여자에게 Private Marketplace 리소스와 설명을 설명하고 업데이트할 수 AWS Marketplace 있는 권한을 부여합니다. AWS Organizations

AWS 관리형 정책: AWSVendorInsightsAssessorFullAccess

AWSVendorInsightsAssessorFullAccess 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 권한 있는 AWS Marketplace Vendor Insights 리소스를 보고 AWS Marketplace Vendor Insights 구독을 관리할 수 있는 전체 액세스 권한을 부여합니다. 이러한 요청은 관리자가 승인하거나 거부해야 합니다. AWS Artifact 타사 보고서를 볼 수 있는 읽기 전용 액세스를 허용합니다.

AWS Marketplace Vendor Insights는 평가자가 구매자와 동일하고 공급업체가 판매자와 동일하다는 것을 식별합니다.

권한 세부 정보

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Action": [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws-marketplace:AgreementType": "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
         "artifact:GetReport",
         "artifact:GetReportMetadata",
         "artifact:GetTermForReport",
         "artifact:ListReports"
      ],
```

```
      "Resource": "arn:aws:artifact:*::report/*"
    }
  ]
}
```

AWS 관리형 정책: AWSVendorInsightsAssessorReadOnly

AWSVendorInsightsAssessorReadOnly 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 권한 있는 AWS Marketplace Vendor Insights 리소스를 볼 수 있는 읽기 전용 액세스 권한을 부여합니다. 이러한 요청은 관리자가 승인하거나 거부해야 합니다. AWS Artifact의 보고서를 볼 수 있는 읽기 전용 액세스를 허용합니다.

요청은 관리자가 승인하거나 거부해야 합니다. AWS Artifact 타사 보고서를 볼 수 있는 읽기 전용 액세스를 허용합니다.

AWS Marketplace Vendor Insights는 이 가이드의 목적상 평가자를 구매자로 식별하고 공급업체가 판매자와 동등하다고 식별합니다.

권한 세부 정보

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "artifact:GetReport",
         "artifact:GetReportMetadata",
         "artifact:GetTermForReport",
         "artifact:ListReports"
      ],
      "Resource": "arn:aws:artifact:*::report/*"
    }
```

```
  ]
}
```

AWS 관리형 정책으로 AWS Marketplace 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후부터 AWS Marketplace의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 AWS Marketplace 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSServiceRoleForPrivateMarketplaceAdminPolicy - AWS Marketplace에 새 기능에 대한 정책이 추가되었습니다.	AWS MarketplacePrivate Marketplace 리소스 관리 및 설명을 AWS Organizations 지원하는 새 정책이 추가되었습니다.	2024년 2월 16일
AWSPrivateMarketplaceAdminFullAccess - 기존 정책에 대한 업데이트	AWS MarketplaceAWS Organizations데이터 읽기를 지원하도록 정책을 업데이트했습니다.	2024년 2월 16일
AWSMarketplaceDeploymentServiceRolePolicy - AWS Marketplace에 새 기능에 대한 정책이 추가되었습니다.	AWS Marketplace에서 배포 관련 파라미터 관리를 지원하는 새 정책을 추가했습니다.	2023년 11월 29일
AWSMarketplaceRead기존 정책에 대한 업데이트만 해당 및 AWSMarketplaceManageSubscriptions—	AWS Marketplace에서는 비공개 제안 페이지에 대한 액세스를 허용하도록 기존 정책을 업데이트했습니다.	2023년 1월 19일
AWSPrivateMarketplaceAdminFullAccess - 기존 정책에 대한 업데이트	AWS Marketplace에서는 새로운 태그 기반 권한 부여 기능에 대한 정책을 업데이트했습니다.	2022년 12월 9일
AWSVendorInsightsAssessorReadOnlyAWS	AWS Marketplace에서는 AWSVendorInsightsA	2022년 11월 30일

변경 사항	설명	날짜
Marketplace업데이트됨 AWSVendorInsightsAssessorReadOnly	ssessorReadOnly 를 업데이트하여 AWS Artifact 타사 보고서의 보고서에 대한 읽기 전용 액세스(미리 보기)를 추가했습니다.	
AWSVendorInsightsAssessorFullAccessAWS Marketplace업데이트되었습니다 AWSVendorInsightsAssessorFullAccess	AWS Marketplace에서는 AWSVendorInsightsAssessorFullAccess 를 업데이트하여 계약 검색 기능과 AWS Artifact 타사 보고서에 대한 읽기 전용 액세스(미리 보기)를 추가했습니다.	2022년 11월 30일
AWSVendorInsightsAssessorFullAccess및 AWSVendorInsightsAssessorReadOnly— 새 기능에 대한 정책 추가 AWS Marketplace	AWS Marketplace에서는 AWS Marketplace Vendor Insights의 새 기능인 AWSVendorInsightsAssessorFullAccess 및 AWSVendorInsightsAssessorReadOnly 에 대한 정책을 추가했습니다.	2022년 7월 26일
AWSMarketplaceFullAccess 및 AWSMarketplaceImageBuildFullAccess - 기존 정책 업데이트	AWS Marketplace에서는 보안 강화를 위해 더 이상 필요 없는 권한을 제거했습니다.	2022년 3월 4일
AWSPrivateMarketplaceAdminFullAccess - 기존 정책 업데이트	AWS Marketplace에서는 AWSPrivateMarketplaceAdminFullAccess 정책에서 사용되지 않은 권한을 제거했습니다.	2021년 8월 27일

변경 사항	설명	날짜
AWSMarketplaceFullAccess-기존 정책 업데이트	AWS Marketplace에서는 `AWSMarketplaceFullAccess` 정책에서 중복되는 `ec2:DescribeAccountAttributes` 권한을 제거했습니다.	2021년 7월 20일
AWS Marketplace에서 변경 사항 추적 시작	AWS Marketplace이(가) AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2021년 4월 20일

고객 지원에 필요한 AWS 계정 번호 찾기

구매자 또는 구매자의 사용자가 AWS Support에 문의해야 하는 경우 AWS 계정 번호가 필요합니다.

AWS 계정 번호를 찾는 방법

1. 사용자 이름으로 AWS Management Console에 로그인합니다.
2. 상단 탐색 모음에서 지원을 선택한 후 지원 센터를 선택합니다.

AWS 계정 ID(계정 번호)는 상단 탐색 모음 아래에 표시됩니다.

AWS Marketplace에 서비스 연결 역할 사용

AWS Marketplace는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 링크 역할은 AWS Marketplace에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 링크 역할은 AWS Marketplace에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

주제

- 역할을 사용하여 AWS Marketplace에 대한 권한 공유
- AWS Marketplace에서 역할을 사용하여 구매 주문 작업
- 역할을 사용하여 AWS Marketplace 제품 구성 및 실행
- 역할을 사용하여 프라이빗 마켓플레이스 구성 AWS Marketplace

역할을 사용하여 AWS Marketplace에 대한 권한 공유

AWS Marketplace는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 AWS Marketplace에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS Marketplace에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 통해 AWS Marketplace 설정이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. AWS Marketplace에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 AWS Marketplace에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 이 권한 정책은 다른 어떤 IAM 엔터티에도 연결할 수 없습니다.

AWS License Manager를 사용하여 AWS 조직의 다른 계정과 AWS Marketplace 구독을 공유하려면 공유하려는 각 계정에 대한 AWS Marketplace 권한을 부여해야 합니다. AWSServiceRoleForMarketplaceLicenseManagement 역할을 사용하면 됩니다. 자세한 내용은 AWS Marketplace에 대한 서비스 연결 역할 생성 섹션을 참조하세요.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스 섹션에서 서비스 연결 역할 열이 예인 서비스를 찾아보세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS Marketplace에 대한 서비스 연결 역할 권한

AWS Marketplace에서는 AWSServiceRoleForMarketplaceLicenseManagement라는 서비스 연결 역할을 사용합니다. 이 역할은 AWS Marketplace에서 구독하는 제품에 대한 라이선스를 AWS License Manager에서 생성하고 관리할 수 있는 권한을 AWS Marketplace에 부여합니다.

AWSServiceRoleForMarketplaceLicenseManagement 서비스 연결 역할은 다음 서비스가 구매자 대신 License Manager에서 작업을 수행하는 것을 신뢰합니다.

- `license-management.marketplace.amazonaws.com`

이름이 AWSMarketplaceLicenseManagementServiceRolePolicy인 연결 권한 정책은 AWS Marketplace가 지정된 리소스에 대해 다음 작업을 수행하는 것을 허용합니다.

- 작업:
  - `"organizations:DescribeOrganization"`
  - `"license-manager:ListReceivedGrants"`
  - `"license-manager:ListDistributedGrants"`

  - "license-manager:GetGrant"
  - "license-manager:CreateGrant"
  - "license-manager:CreateGrantVersion"
  - "license-manager:DeleteGrant"
  - "license-manager:AcceptGrant"
- 리소스:
  - 모든 리소스("*")

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS Marketplace에 대한 서비스 연결 역할 생성

구매자가 AWS License Manager와의 통합을 설정하면 AWS Marketplace는 서비스 연결 역할을 생성합니다.

구매자는 AWS Marketplace가 조직의 모든 계정에 대한 서비스 연결 역할을 한꺼번에 생성하도록 지정하거나, 한 계정에 대한 서비스 연결 역할을 한꺼번에 생성할 수 있습니다. 모든 계정에서 서비스 연결 역할을 생성하는 옵션은 조직에서 모든 기능을 활성화한 경우에만 사용할 수 있습니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.

모든 계정에서 서비스 연결 역할을 생성하는 방법

1. AWS Marketplace 콘솔에 로그인하고 설정을 선택합니다.
2. AWS Organizations 통합 섹션에서 통합 생성을 선택합니다.
3. AWS Organizations 통합 생성 페이지에서 조직 전체에서 신뢰할 수 있는 액세스 활성화를 선택하고 통합 생성을 선택합니다.

> **Note**
>
> 이 설정은 AWS Organizations 내에서 신뢰를 활성화합니다. 따라서 현재 작업 외에도 향후 조직에 추가되는 계정에는 서비스 연결 역할이 자동으로 추가됩니다.

현재 계정에 대한 서비스 연결 역할을 생성하는 방법

1. AWS Marketplace 콘솔에 로그인하고 설정을 선택합니다.

2. AWS Organizations 통합 섹션에서 통합 구성을 선택합니다.
3. AWS Organizations 통합 생성 페이지에서 이 계정의 AWS Marketplace 라이선스 관리 서비스 연결 역할을 선택하고 통합 생성을 선택합니다.

> **Important**
>
> 현재 계정에 대한 서비스 연결 역할만 생성하도록 선택하면 조직 전체에서 신뢰할 수 있는 액세스가 활성화되지 않습니다. AWS Marketplace에서 라이선스를 공유(제공 또는 취득)하려는 계정마다 이 단계를 반복해야 합니다. 나중에 조직에 추가되는 계정도 여기에 포함됩니다.

AWS Marketplace에 대한 서비스 연결 역할 편집

AWS Marketplace에서는 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 객체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AWS Marketplace에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려 할 때 AWS Marketplace 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWSServiceRoleForMarketplaceLicenseManagement 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용자 설명서의 서비스 연결 역할 삭제 섹션을 참조하세요.

AWS Marketplace 서비스 연결 역할이 지원되는 리전

AWS Marketplace에서는 서비스를 사용할 수 있는 모든 AWS 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS Marketplace 리전 및 엔드포인트 섹션을 참조하세요.

AWS Marketplace에서 역할을 사용하여 구매 주문 작업

AWS Marketplace는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 링크 역할은 AWS Marketplace에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS Marketplace에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 직접적으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 통해 AWS Marketplace 설정이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. AWS Marketplace에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 AWS Marketplace에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 AWS Marketplace 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할(Service-linked roles) 열에 예(Yes)가 있는 서비스를 찾으세요. 해당 서비스에 대한 서비스 링크 역할 설명서를 보려면 예 링크를 선택합니다.

AWS Marketplace에 대한 서비스 링크 역할 권한

AWS Marketplace라는 서비스 연결 역할을 사용합니다.
AWSServiceRoleForMarketplacePurchaseOrders— 이 역할은 AWS Marketplace 구독에 구매 주문 번호를 첨부할 수 있는 AWS Marketplace 권한을 제공합니다. AWS Billing and Cost Management

AWSServiceRoleForMarketplacePurchaseOrders 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `purchase-orders.marketplace.amazonaws.com`

이름이 지정된 역할 권한 정책을 AWSMarketplacePurchaseOrdersServiceRolePolicy사용하면 지정된 리소스에서 다음 작업을 AWS Marketplace 완료할 수 있습니다.

- 작업: `"*"`에 대한 `"purchase-orders:ViewPurchaseOrders", "purchase-orders:ModifyPurchaseOrders"`

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하십시오.

AWS Marketplace에 대한 서비스 링크 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 구매자가 AWS Marketplace와의 통합을 설정하면 AWS Billing and Cost Management에서 자동으로 서비스 연결 역할을 생성합니다.

> **Note**
>
> AWS Organizations 내에서 이 설정은 관리 계정에서만 작동합니다. 관리 계정에서 이 절차를 수행해야 합니다. 그러면 조직 내 모든 계정에 대한 서비스 연결 역할 및 구매 주문 지원이 설정됩니다.

서비스 연결 역할 생성

1. AWS Marketplace 콘솔에서 관리 계정에 로그인하고 설정을 선택합니다.
2. AWS 결제 통합 섹션에서 통합 구성을 선택합니다.
3. AWS 결제 통합 생성 페이지에서 조직의 AWS Marketplace 결제 관리 서비스 연결 역할을 선택하고 통합 생성을 선택합니다.

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 구매자가 AWS Marketplace과의 통합을 설정하면 AWS Billing and Cost Management에서 다시 한번 자동으로 서비스 연결 역할을 생성합니다.

AWS Marketplace에 대한 서비스 링크 역할 편집

AWS Marketplace에서는 AWSServiceRoleForMarketplacePurchaseOrders 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하십시오.

AWS Marketplace에 대한 서비스 링크 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할을 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할 수동 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWSServiceRoleForMarketplacePurchaseOrders 서비스 연결 역할을 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제를 참조하십시오.

AWS Marketplace 서비스 링크 역할이 지원되는 리전

AWS Marketplace에서는 서비스를 사용할 수 있는 모든 AWS 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS Marketplace 리전 및 엔드포인트 섹션을 참조하세요.

역할을 사용하여 AWS Marketplace 제품 구성 및 실행

AWS Marketplace는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 AWS Marketplace에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS Marketplace에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 통해 AWS Marketplace 설정이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. AWS Marketplace에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 AWS Marketplace에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS Marketplace에 대한 서비스 연결 역할 권한

AWS Marketplace에서는 AWSServiceRoleForMarketplaceDeployment라는 서비스 연결 역할을 사용하여 AWS Marketplace에서 사용자를 대신하여 AWS Secrets Manager에 보안 정보로 저장되는 배포 관련 파라미터를 관리할 수 있게 합니다. 판매자는 AWS CloudFormation 템플릿에서 이러한 보안 정보를 참조할 수 있으며, AWS Marketplace에서 빠른 시작이 활성화된 제품을 구성할 때 해당 템플릿을 실행할 수 있습니다.

AWSServiceRoleForMarketplaceDeployment 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `deployment.marketplace.amazonaws.com`

이름이 AWSMarketplaceDeploymentServiceRolePolicy인 역할 권한 정책은 AWS Marketplace에서 지정된 리소스에 대해 다음 작업을 완료하도록 허용합니다.

> **Note**
>
> AWS Marketplace 관리형 정책에 대한 자세한 내용은 AWS Marketplace 구매자를 위한 AWS 관리형 정책을 참조하십시오.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ManageMarketplaceDeploymentSecrets",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:CreateSecret",
    "secretsmanager:PutSecretValue",
    "secretsmanager:DescribeSecret",
    "secretsmanager:DeleteSecret",
    "secretsmanager:RemoveRegionsFromReplication"
   ],
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "ListSecrets",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:ListSecrets"
   ],
   "Resource": [
    "*"
   ]
  },
  {
```

```
    "Sid": "TagMarketplaceDeploymentSecrets",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:TagResource"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
    "Condition": {
     "Null": {
      "aws:RequestTag/expirationDate": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": [
       "expirationDate"
      ]
     },
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   }
  ]
}
```

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWS Marketplace에 대한 서비스 연결 역할 생성

서비스 연결 역할 설정은 역할이 존재하는 한 빠른 시작이 활성화된 모든 제품에 대한 권한을 제공하는 일회성 작업입니다.

빠른 시작이 활성화된 제품을 구성하면 AWS Marketplace에서 계정에 필요한 서비스 연결 역할이 생성되었는지 여부를 감지합니다. 역할이 누락된 경우 통합 활성화 버튼이 포함된 AWS Marketplace 배포 파라미터 통합을 활성화하라는 메시지가 표시됩니다. 이 버튼을 선택할 때 AWS Marketplace에서 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이 서비스 연결 역할은 이전에 빠른 시작이 활성화된 제품을 구성했을 경우 계정에 나타납니다. 자세한 내용은 내 AWS 계정 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제하고 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 빠른 시작이 활성화된 제품의 구성 페이지를 열면 통합 활성화 버튼이 표시되며, 이 버튼을 다시 선택하여 서비스 연결 역할을 다시 생성할 수 있습니다.

IAM 콘솔을 사용해 AWS Marketplace - 배포 관리 사용 사례로 서비스 연결 역할을 생성할 수도 있습니다. AWS CLI 또는 AWS API에서 `deployment.marketplace.amazonaws.com` 서비스 이름의 서비스 연결 역할을 생성합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성을 참조하십시오. 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

AWS Marketplace에 대한 서비스 연결 역할 편집

AWS Marketplace에서는 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 객체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AWS Marketplace에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 삭제하려는 역할이 서비스에서 사용되고 있는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하십시오.

`deployment.marketplace.amazonaws.com` 서비스에서 사용하는 AWS Marketplace 리소스를 삭제하려면 SecretsManager에서 모든 Marketplace 배포 관련 보안 정보를 삭제해야 합니다. 다음과 같은 방법으로 관련 보안 정보를 찾을 수 있습니다.

- `marketplace-deployment`에서 관리하는 보안 정보 검색.
- 태그 키 `aws:secretsmanager:owningService`와 값 `marketplace-deployment`를 사용하여 보안 정보 검색.
- 보안 정보 이름 앞에 `marketplace-deployment!` 접두사가 붙은 보안 정보 검색.

IAM을 사용하여 서비스 연결 역할을 삭제하려면

IAM 콘솔, AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForMarketplaceDeployment 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제를 참조하세요.

AWS Marketplace 서비스 연결 역할이 지원되는 리전

AWS Marketplace에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS Marketplace 리전 및 엔드포인트를 참조하십시오.

역할을 사용하여 프라이빗 마켓플레이스 구성 AWS Marketplace

AWS Marketplace은(는) AWS Identity and Access Management(IAM) service-linked roles(서비스 링크 역할)을 사용합니다. 서비스 링크 역할은 AWS Marketplace에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS Marketplace에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 직접적으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 통해 AWS Marketplace 설정이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. AWS Marketplace에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 AWS Marketplace에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 링크 역할 설명서를 보려면 예 링크를 선택합니다.

AWS Marketplace에 대한 서비스 링크 역할 권한

AWS Marketplace는 이름이 지정된 서비스 연결 역할을 사용하여 AWSServiceRoleForPrivateMarketplaceAdminPrivate Marketplace 리소스와 설명을 설명하고 업데이트합니다. AWS Organizations

AWSServiceRoleForPrivateMarketplaceAdmin 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `private-marketplace.marketplace.amazonaws.com`

이름이 AWSServiceRoleForPrivateMarketplaceAdminPolicy지정된 역할 권한 정책을 사용하면 AWS Marketplace 지정된 리소스에서 다음 작업을 수행할 수 있습니다.

> **Note**
>
> AWS Marketplace 관리형 정책에 대한 자세한 내용은 AWS Marketplace구매자를 위한 AWS 관리형 정책을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrivateMarketplaceCatalogDescribePermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeEntity"
            ],
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceCatalogListPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:ListChangeSets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceStartChangeSetPermissions",
            "Effect": "Allow",
```

```
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Condition": {
                "StringEquals": {
                    "catalog:ChangeType": [
                        "AssociateAudience",
                        "DisassociateAudience"
                    ]
                }
            },
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceOrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListChildren"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하십시오.

AWS Marketplace에 대한 서비스 링크 역할 생성

서비스 연결 역할을 수동으로 생성할 필요가 없습니다. 조직의 Private Marketplace를 활성화하면 서비스 연결 역할이 자동으로 AWS Marketplace 생성됩니다.

> **Note**
>
> 이 역할은 의 AWS Organizations 관리 계정에만 필요하며 관리 계정에서만 생성됩니다.

서비스 연결 역할 생성

1. Private Marketplace 시작하기 페이지에서 조직 전체에서 신뢰할 수 있는 액세스를 활성화하는 옵션을 선택하고 Private Marketplace 서비스 연결 역할을 생성합니다. 이러한 옵션은 관리 계정에서만 사용할 수 있습니다.
2. 프라이빗 마켓플레이스 활성화를 선택합니다.

기존 Private Marketplace 고객인 경우 조직 전체에서 신뢰할 수 있는 액세스를 활성화하고 Private Marketplace 서비스 연결 역할을 활성화하는 옵션을 프라이빗 마켓플레이스 관리 대시보드의 설정 페이지에서 사용할 수 있습니다.

이 서비스 연결 역할을 삭제하고 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다.

AWS Marketplace에 대한 서비스 링크 역할 편집

AWS Marketplace에서는 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하십시오.

AWS Marketplace에 대한 서비스 링크 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없어야 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할을 삭제하려면 먼저 다음을 수행해야 합니다.

- 조직 전체에서 신뢰할 수 있는 액세스를 비활성화하세요.
- 모든 프라이빗 마켓플레이스 경험을 분리하세요.

IAM을 사용하여 수동으로 서비스 링크 역할을 삭제하려면

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWSServiceRoleForPrivateMarketplaceAdmin 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용자 설명서의 서비스 연결 역할 삭제 섹션을 참조하세요.

AWS Marketplace 서비스 링크 역할이 지원되는 리전

AWS Marketplace에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 링크 역할 사용을 지원합니다. 자세한 내용은 AWS Marketplace 리전 및 엔드포인트를 참조하십시오.

프라이빗 마켓플레이스 관리자 생성

관리자 그룹을 생성하여 회사의 프라이빗 마켓플레이스 설정을 관리할 수 있습니다. 조직에서 프라이빗 마켓플레이스를 활성화하면 프라이빗 마켓플레이스의 관리자가 다음을 비롯한 다양한 작업을 수행할 수 있습니다.

- 경험과 잠재고객을 보고 만들 수 있습니다.
- 프라이빗 마켓플레이스 경험에 제품을 추가합니다.
- 프라이빗 마켓플레이스 경험에서 제품을 제거합니다.
- 프라이빗 마켓플레이스 경험의 사용자 인터페이스를 구성합니다.
- 프라이빗 마켓플레이스 경험을 활성화 및 비활성화합니다.
- AWS Marketplace Catalog API를 호출하여 프라이빗 마켓플레이스 경험을 프로그래밍 방식으로 관리합니다.

각 관리자의 권한이 하위 작업 세트로 제한되는 프라이빗 마켓플레이스 관리자를 여러 명 생성하려면 the section called “프라이빗 마켓플레이스 관리자를 위한 사용자 지정 정책 생성” 섹션을 참조하세요.

> **Note**
>
> 프라이빗 마켓플레이스를 활성화하려면 관리 계정에서 한 번만 실행해야 합니다. 자세한 내용은 프라이빗 마켓플레이스 시작하기를 참조하십시오.

the section called “AWSPrivateMarketplaceAdminFullAccess”를 사용자, 그룹 또는 역할에 연결하여 프라이빗 마켓플레이스를 관리할 수 있는 AWS Identity and Access Management(IAM) 권한을 부여합니다. 그룹 또는 역할을 사용하는 것이 좋습니다. 정책을 연결하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 사용자 그룹에 정책 연결을 참조하세요.

AWSPrivateMarketplaceAdminFullAccess 정책의 권한에 대한 자세한 내용은 the section called "AWSPrivateMarketplaceAdminFullAccess" 섹션을 참조하세요. AWS Marketplace에서 사용할 수 있는 다른 정책에 대해 알아보려면 AWS Management Console에 로그인하고 IAM 정책 페이지로 이동합니다. 검색 상자에 **Marketplace**를 입력하여 AWS Marketplace와 관련된 모든 정책을 찾습니다.

프라이빗 마켓플레이스 관리자를 위한 사용자 지정 정책 생성

조직에서는 각 관리자의 권한이 하위 작업 세트로 제한되는 프라이빗 마켓플레이스 관리자를 여러 명 생성할 수 있습니다. AWS Identity and Access Management(IAM) 정책을 튜닝하여 AWS Marketplace 카탈로그에 사용되는 작업, 리소스 및 조건 키에 나열된 AWS Marketplace Catalog API 작업에 대한 조건 키와 리소스를 지정할 수 있습니다. AWS Marketplace Catalog API변경 유형 및 리소스를 사용하여 IAM 정책을 조정하는 일반적인 메커니즘은 AWSMarketplace Catalog API 가이드에 설명되어 있습니다. 프라이빗 AWS Marketplace에서 사용할 수 있는 모든 변경 유형 목록은 프라이빗 마켓플레이스 작업을 참조하세요.

고객 관리형 정책을 생성하려면 IAM 정책 생성을 참조하세요. 다음은 프라이빗 마켓플레이스에 제품을 추가 또는 제거하는 것만 가능한 관리자를 생성하는 데 사용할 수 있는 정책 JSON 예시입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:ListEntities",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Condition": {
                "StringEquals": {
                    "catalog:ChangeType": [
                        "AllowProductProcurement",
                        "DenyProductProcurement"
                    ]
                }
            },
            "Resource": "*"
        }
    ]
}
```

프라이빗 마켓플레이스 리소스의 하위 집합을 관리하도록 정책을 제한할 수도 있습니다. 다음은 특정 프라이빗 마켓플레이스 경험만 관리할 수 있는 관리자를 생성하는 데 사용할 수 있는 정책 JSON 예시입니다. 이 예제에서는 `Experience` 식별자가 `exp-1234example`인 리소스 문자열을 사용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
```

```
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/exp-1234example"
            ]
        }
    ]
}
```

엔터티 식별자를 검색하는 방법과 프라이빗 마켓플레이스 리소스 세트를 보는 방법에 대한 자세한 내용은 프라이빗 마켓플레이스 작업을 참조하세요.

문서 기록

다음 표에서는 AWS Marketplace 구매자 설명서의 이번 릴리스를 소개합니다.

이 설명서가 업데이트될 때 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
지원 정책이 업데이트되었습니다. AWS Organizations	AWS Organizations데이터 읽기 액세스를 `AWSPrivateMarketplaceAdminFullAccess` 허용하도록 관리형 정책을 업데이트했습니다.	2024년 2월 16일
AWS Marketplace의 제품에 대한 새로운 서비스 연계 역할	AWS Marketplace이제 Private Marketplace 리소스를 설명 및 업데이트하고 설명하는 서비스 연결 역할을 제공합니다. AWS Organizations	2024년 2월 16일
새로운 프라이빗 마켓플레이스 경험 시작 AWS Marketplace	AWS Marketplace이제 프라이빗 마켓플레이스 경험을 관리할 위임된 관리자와의 통합 AWS Organizations 및 등록 기능을 지원합니다.	2024년 2월 16일
AWS Marketplace의 미래 날짜의 계약에 대한 일반 가용성	이제 모든 SaaS ISV 및 채널 파트너를 위한 미래 날짜의 계약 기능을 AWS Marketplace에서 정식 버전으로 사용할 수 있습니다. 미래 날짜의 계약을 사용하면 고객은 운영 노력을 줄여 동일한 제품 목록에서 기존 구매 내역이 있는 경우 거래를 미리 예약하거나 갱신을 설정할 수 있습니다.	2024년 1월 16일

캐나다 서부(캘거리) 지역 지원	AWS Marketplace에서는 이제 캐나다 서부(캘거리) AWS 리전을 지원합니다.	2023년 12월 20일
AWS Marketplace의 제품에 대한 새로운 서비스 연계 역할	AWS Marketplace에서는 이제 구매자를 대신하여 AWS Secrets Manager에 보안 정보로 저장되는 배포 관련 파라미터를 관리할 수 있는 서비스 연결 역할을 제공합니다.	2023년 11월 29일
구매자를 위한 새로운 빠른 시작 배포 옵션	이제 구매자는 AWS Marketplace에서 적용 가능한 SaaS(Software as a Service) 제품을 구성, 배포 및 시작하는 데 필요한 시간, 리소스 및 단계를 줄일 수 있습니다.	2023년 11월 29일
비공개 제안에 대한 유연한 결제 일정이 제공됩니다.	이제 AWS Marketplace의 모든 고객이 비공개 제안에 대한 유연한 결제 일정(FPS)을 이용할 수 있습니다.	2023년 11월 17일
Amazon EKS의 타사 추가 기능	이제 고객은 AWS Marketplace로 리디렉션되지 않고 Amazon EKS 콘솔에서 타사 추가 기능을 구독할 수 있습니다.	2023년 10월 18일
아마존 지원 EventBridge	AWS Marketplace이전에는 아마존 이벤트라고 불렸던 EventBridge 아마존과 통합되었습니다. CloudWatch	2023년 9월 6일
이스라엘(텔아비브) 리전 지원	AWS Marketplace에서 이제 이스라엘(텔아비브) AWS 리전을 지원합니다.	2023년 8월 1일

AMI 연간 계약의 구매 주문 지원	이제 AWS Marketplace에서는 Amazon Machine Image(AMI) 연간 계약의 구매 주문 기능을 지원합니다.	2023년 6월 29일
AWS Billing 콘솔에서 구매 주문 가능	이제 구매자는 AWS Billing 콘솔에서 모든 구매 주문을 관리하고 out-of-cycle SaaS 계약 PDF 송장을 해당 구매 주문과 쉽게 조정할 수 있습니다.	2023년 2월 3일
아시아 태평양(멜버른) 리전 지원	이제 AWS Marketplace에서는 아시아 태평양(멜버른) AWS 리전을 지원합니다.	2023년 1월 24일
비공개 제안 페이지에 대한 정책 업데이트	비공개 제안 페이지에 대한 액세스를 허용하도록 관리형 정책 `AWSMarketplaceRead-only` 및 `AWSMarketplaceManageSubscriptions` 를 업데이트했습니다.	2023년 1월 19일
비공개 제안 페이지	인증된 구매자는 이제 비공개 제안 페이지에서 자신의 AWS 계정에 제시된 AWS Marketplace 비공개 제안을 볼 수 있습니다.	2023년 1월 19일
구매자를 위한 이메일 알림 업데이트	이제 비공개 제안이 게시되면 구매자에게 알림이 전송됩니다.	2022년 12월 22일
이제 AWS Marketplace의 구매자는 구독의 SaaS 무료 평가판 사용 가능	이제 구매자는 구독 SaaS 제품의 무료 평가판을 구독할 수 있습니다.	2022년 12월 16일

구매자는 SaaS 비공개 제안 업그레이드 또는 갱신을 수락 가능	판매자가 이전 SaaS 비공개 제안을 업그레이드 또는 갱신한 경우 구매자는 기존 계약을 취소할 필요 없이 새 비공개 제안을 수락할 수 있습니다.	2022년 12월 13일
AWS Marketplace에서 프라이빗 마켓플레이스 경험 보관 가능	이제 구매자는 AWS Marketplace에서 프라이빗 마켓플레이스 경험을 보관하고 다시 활성화할 수 있습니다.	2022년 12월 12일
AWS Marketplace 태그 기반 권한 부여 기능에 대한 정책 업데이트	AWS Marketplace에서 태그 기반 인증을 지원하도록 `AWSPrivateMarketplaceAdminFullAccess` 정책을 업데이트했습니다.	2022년 12월 9일
구독 취소 방법에 대한 정보를 제공하는 새 주제 추가	AWS Marketplace에서 AMI, ML 및 SaaS 제품 구독을 취소하는 방법에 대한 정보가 추가되었습니다. SaaS 계약의 자동 갱신 취소에 대한 정보도 추가되었습니다.	2022년 12월 8일
AWS Marketplace Vendor Insights의 구매자를 위한 정책 업데이트	AWS Marketplace Vendor Insights 구매자를 위한 `AWSVendorInsightsAssessorFullAccess` 및 `AWSVendorInsightsAssessorReadOnly` 관리형 정책이 업데이트되었습니다.	2022년 11월 30일
AWS Marketplace Vendor Insights 구매자의 액세스 권한 제어	구매자에게 허용되는 작업과 권한을 설명하는 새 주제가 AWS Marketplace Vendor Insights에 추가되었습니다.	2022년 11월 30일

아시아 태평양(하이데라바드) 리전 지원	이제 AWS Marketplace에서는 아시아 태평양(하이데라바드) AWS 리전을 지원합니다.	2022년 11월 22일
유럽(스페인) 리전 지원	이제 AWS Marketplace에서는 유럽(스페인) AWS 리전을 지원합니다.	2022년 11월 16일
유럽(취리히) 리전 지원	이제 AWS Marketplace에서는 유럽(취리히) AWS 리전을 지원합니다.	2022년 11월 9일
2022년 12월까지 AWS Marketplace 웹 사이트를 IPv6로 업그레이드	현재 IAM 정책에서 IPv4 형식 주소를 사용하는 구매자는 2022년 12월 15일 전까지 IAM 정책을 IPv6 형식 주소로 업데이트하는 것이 좋습니다.	2022년 9월 29일
AWS Marketplace 프라이빗 마켓플레이스 세분화 권한	이제 구매자는 프라이빗 마켓플레이스 경험을 관리할 수 있는 보다 세분화된 권한을 갖게 되었습니다.	2022년 9월 8일
AWS Marketplace Vendor Insights에 대한 두 가지 정책 추가	소프트웨어 위험 평가를 제공하는 기능인 AWS Marketplace Vendor Insights에 대한 `AWSVendorInsightsAssessorFullAccess` 및 `AWSVendorInsightsAssessorReadOnly` 정책이 추가되었습니다.	2022년 7월 26일
AWS Marketplace Vendor Insights	AWS Marketplace Vendor Insights는 소프트웨어 위험 평가를 제공하는 기능입니다.	2022년 7월 26일

결제 방법 업데이트	AWS 결제 콘솔에서 결제 방법을 변경하는 방법을 명확히 하기 위해 설명서만 업데이트했습니다.	2022년 6월 1일
계약용 SaaS 무료 평가판	이제 구매자는 계약용 SaaS 무료 평가판을 구독하여 제품을 살펴본 후 유료 평가판으로 전환할 수 있습니다.	2022년 5월 31일
AMI, 컨테이너 및 SaaS 제품에 대한 공급업체 측정 태그 추가	공급업체에서 제공한 지표 전반의 AWS Marketplace 리소스 사용량을 고객이 이해하는 데 도움이 되는 태그를 제공하는 새로운 기능입니다.	2022년 5월 27일
구매자 트랜잭션에 이메일 알림 추가	AWS Marketplace에서 이루어진 계약을 확인하는 이메일 알림을 구매자에게 보내는 새 기능입니다.	2022년 5월 23일
eProcurement 고객을 위한 무료 제품 및 BYOL 제품의 자동 승인 활성화	고객은 eProcurement 고객을 위한 무료 제품 및 BYOL 제품의 새 자동 승인 기능을 통해 제품을 즉시 사용할 수 있습니다.	2022년 5월 2일
AMI 및 컨테이너 제품 계약 구매자의 계약 수정 활성화	AMI 및 컨테이너 제품 계약을 수정하여 추가 권한을 구매하거나 자동 구독 갱신 옵션을 활성화할 수 있습니다.	2022년 4월 6일
라이선스 사용 추적 기능	이제 구매자는 AWS License Manager를 사용하여 AMI 및 SaaS 제품에 대한 사용량 기반 라이선스 지표를 추적할 수 있습니다.	2022년 3월 28일

Helm CLI 버전 업데이트	Helm CLI 버전이 3.7.0에서 3.7.1로 변경된 것과 관련하여 컨테이너 제품 설명서가 업데이트되었습니다. 현재 호환되는 버전은 이 버전뿐입니다.	2022년 3월 8일
기존 관리형 정책 업데이트	더 이상 필요 없는 권한이 `AWSMarketplaceFullAccess` 및 `AWSMarketplaceImageBuildFullAccess` 정책에서 제거되었습니다.	2022년 3월 4일
EMEA 거주 구매자가 Amazon Web Services EMEA SARL을 통해 제품 구매 가능	AWS 계정 위치가 터키와 남아프리카 공화국을 제외한 유럽, 중동 및 아프리카(EMEA) 국가와 지역인 AWS Marketplace 구매자는 이제 Amazon Web Services EMEA SARL을 통해 EMEA 적격 판매자로부터 구매한 제품에 대한 AWS Marketplace 인보이스를 받을 수 있습니다.	2022년 1월 7일
아시아 태평양(자카르타) 리전 지원	이제 AWS Marketplace에서는 아시아 태평양(자카르타) AWS 리전을 지원합니다.	2021년 12월 13일
컨테이너 기반 제품의 차트 Helm 제공 방법	이제 구매자는 시작 환경에 차트 Helm을 설치하여 컨테이너 기반 제품을 시작할 수 있습니다.	2021년 11월 29일

컨테이너 기반 제품 설명서의 일반 업데이트 및 재구성	컨테이너 기반 제품 설명서를 업데이트하여 컨테이너 기반 제품의 검색, 구독 및 시작에 대한 정보를 더 추가하고 명확히 했습니다.	2021년 11월 29일
에 대한 설명서가 추가되었습니다. QuickLaunch	구매자는 이제 헬름 차트 전달 방법을 사용하여 컨테이너 기반 제품을 QuickLaunch 출시할 때 사용할 수 있습니다. QuickLaunch 는 새 Amazon EKS 클러스터를 빠르게 생성하고 AWS Marketplace 해당 클러스터에서 컨테이너 기반 애플리케이션을 시작하는 AWS CloudFormation 데 활용하는 기능입니다.	2021년 11월 29일
AMI 기반 제품과 컨테이너 기반 제품의 계약 요금	구매자는 이제 선결제 요금으로 AMI 기반 제품 또는 컨테이너 기반 제품을 구매할 수 있습니다.	2021년 11월 17일
SaaS 제품의 구매 주문 지원	AWS Marketplace에서 서비스형 소프트웨어(SaaS) 계약 구매에 구매 주문 번호를 추가할 수 있습니다.	2021년 10월 28일
SAP Ariba 통합 지원	AWS Marketplace에서 SAP Ariba 조달 시스템과의 통합을 지원합니다.	2021년 10월 13일
AMI 별칭 지원	AWS Marketplace에서는 모든 리전에서 사용할 수 있는 AMI ID의 별칭 사용을 지원합니다.	2021년 9월 8일

관리형 정책에서 사용되지 않은 권한 제거	`AWSPrivateMarketplaceAdminFullAccess` AWS 관리형 정책에서 사용되지 않은 권한이 제거되었습니다.	2021년 8월 27일
AWS License Manager를 통한 라이선스 공유 지원	구매한 제품의 라이선스를 AWS 조직의 다른 계정과 공유할 수 있습니다.	2020년 12월 3일
AWS Marketplace에서 전문 서비스 제품 지원	이제 AWS Marketplace에서 전문 서비스를 구매할 수 있습니다.	2020년 12월 3일
기본 통화 지원	AWS Marketplace 구매 대금을 기본 통화로 결제할 수 있습니다.	2020년 7월 27일
구매자는 비공개 제안 업그레이드 및 갱신을 검토하고 수락할 수 있습니다.	판매자는 SaaS 계약 및 소비 제품이 포함된 SaaS 계약에 대한 업그레이드 및 갱신 비공개 제안을 제공할 수 있으며, 구매자는 기존 계약을 사용하는 동안 이를 검토하고 수락할 수 있습니다.	2020년 5월 28일
AWS Marketplace는 AWS Data Exchange를 통해 데이터 제품 지원	이제 AWS Marketplace의 AWS Data Exchange 데이터 제품을 구독할 수 있습니다.	2019년 11월 13일
AWS Marketplace, 시간당 지불 컨테이너 지원	이제 AWS Marketplace는 Amazon Elastic Kubernetes Service(Amazon EKS)에서 실행되는 시간당 유료 컨테이너를 지원합니다.	2019년 9월 25일

AWS Marketplace의 비공개 제안 업데이트	여러 유형의 비공개 제안 수락에 대한 자세한 내용을 제공하도록 콘텐츠가 업데이트됨.	2019년 3월 29일
AWS Marketplace에 대한 보안 업데이트	IAM 정책 정보를 업데이트하고, 가독성 향상을 위해 섹션을 재구성했습니다.	2019년 3월 25일
프라이빗 마켓플레이스 기능에 대한 콘텐츠 추가	프라이빗 마켓플레이스의 릴리스를 지원하는 콘텐츠가 추가됨.	2018년 11월 27일
구매자용 사용 설명서의 최초 릴리스	AWS Marketplace 구매자 설명서가 처음으로 공개되었습니다.	2018년 11월 16일

AWS 용어집

최신 AWS 용어는 참조의 AWS 용어집을 참조하십시오.AWS 용어집

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