사용자 가이드

# AWS Artifact

# AWS Artifact: 사용자 가이드

# Table of Contents

# AWS Artifact란 무엇인가요?

AWS Artifact 는 AWS 보안 및 규정 준수 문서의 온디맨드 다운로드를 제공합니다. 예를 들어, 국제 표준화 기구(ISO) 표준 및 결제 카드 산업(PCI) 보안 표준 및 시스템 및 조직 제어(SOC) 보고서 준수에 대한 보고서입니다. AWS Artifact 또한 는 AWS 보안 제어의 구현 및 운영 효율성을 검증하는 인증 기관의 인증 다운로드를 제공합니다.

를 사용하면 에서 제품을 판매하는 독립 소프트웨어 공급업체(ISVs)에 대한 보안 및 규정 준수 문서를 다운로드할 AWS Artifact수도 있습니다 AWS Marketplace. 자세한 내용은 AWS Marketplace 공급업체 통찰력을 참조하십시오.

또한 AWS Artifact 를 사용하여 조직의 여러 에 AWS 대해 및 와 체결한 계약의 상태를 검토, 수락 AWS 계정 및 추적할 수 AWS 계정 있습니다. 의 계약에 대한 자세한 내용은 섹션을 AWS Artifact참조하세요에서 계약 관리 AWS Artifact.

사용하는 AWS 인프라 및 서비스의 보안 및 규정 준수를 입증하기 위해 감사 아티팩트 로 감사자 또는 규제 기관에 AWS Artifact 문서를 제출할 수 있습니다.  또한 이러한 감사 아티팩트를 지침으로 사용하여 자체 클라우드 아키텍처를 평가하고 회사 내부 제어의 효율성을 평가할 수 있습니다. 감사 아티팩트에 대한 자세한 내용은 AWS Artifact 섹션을 FAQs참조하세요.

> **Note**
>
> AWS 고객은 회사의 보안 및 규정 준수를 입증하는 문서를 개발하거나 획득할 책임이 있습니다. 자세한 내용은 공동 책임 모델을 참조하세요.

## 요금

AWS 는 AWS Artifact 문서 및 계약을 무료로 제공합니다.

# 시작하기 AWS Artifact

사용을 시작하려면 AWS Artifact 콘솔에서 주요 기능을 AWS Artifact사용해 보세요. 콘솔에서 AWS 보안 및 규정 준수 보고서를 다운로드하고, 법적 계약을 다운로드 및 수락하고, AWS Artifact 문서에 대한 알림을 구독할 수 있습니다.

## 사전 조건

의 기능을 사용하려면 가 있어야 AWS Artifact합니다 AWS 계정. 설정 지침은 AWS 설정 사용 설명서의 새 설정을 참조하세요 AWS 계정.

## 특성

의 기능 사용에 대한 지침은 다음 주제를 AWS Artifact참조하세요.

- 보고서 다운로드
- 계약 관리
- 알림 구성

# 에서 보고서 다운로드 AWS Artifact

AWS Artifact 콘솔에서 보고서를 다운로드할 수 있습니다. 에서 보고서를 다운로드하면 AWS Artifact 보고서가 특별히 생성되며 모든 보고서에는 고유한 워터마크가 있습니다. 따라서 신뢰할 수 있는 사람과만 보고서를 공유해야 합니다. 보고서를 이메일에 첨부하여 보내거나 온라인으로 공유하지 마십시오. 보고서를 공유하려면 Amazon 과 같은 보안 공유 서비스를 사용합니다 WorkDocs. 일부 보고서를 다운로드하려면 먼저 이용 약관에 동의해야 합니다.

내용



## 보고서 다운로드

보고서를 다운로드하려면 필요한 권한이 있어야 합니다. 자세한 내용은 의 자격 증명 및 액세스 관리 AWS Artifact 단원을 참조하십시오.

에 가입하면 AWS Artifact계정에 일부 보고서를 다운로드할 수 있는 권한이 자동으로 부여됩니다. 에 액세스하는 데 문제가 있는 경우 AWS Artifact 서비스 승인 참조 페이지의 지침을 AWS Artifact따르세요.

보고서 다운로드

1. 에서 AWS Artifact 콘솔을 엽니다https://console.aws.amazon.com/artifact/.
2. AWS Artifact 홈 페이지에서 보고서 보기를 선택합니다.

   보고서 페이지의 AWS 보고서 탭에서 AWS 보고서에 액세스할 수 있습니다(예: SOC 1/2/3, PCI, C5 등). 타사 보고서 탭에서 에서 제품을 판매하는 독립 소프트웨어 공급업체(ISVs)의 보고서에 액세스할 수 있습니다 AWS Marketplace.
3. (선택 사항) 보고서를 찾으려면 검색 필드에 키워드를 입력합니다. 보고서 제목, 범주, 시리즈 및 설명을 포함하여 개별 열을 기반으로 보고서를 대상으로 검색할 수도 있습니다. 예를 들어 클라우드 컴퓨팅 규정 준수 제어 카탈로그(C5) 보고서를 찾으려면 '제목', '포함' 연산자(:) 및 'C5'()라는 용어를 사용하여 제목 열을 검색할 수 있습니다**`Title : C5`**.

4. (선택 사항) 보고서에 대한 자세한 내용을 보려면 보고서의 제목을 선택하여 세부 정보 페이지를 엽니다.
5. 보고서를 선택하고 보고서 다운로드를 선택합니다.
6. 다운로드하려는 특정 보고서에 대한 사용 약관(보고서 다운로드에 대한 조건 수락)을 수락하라는 메시지가 표시될 수 있습니다. 이용 약관을 자세히 읽어보는 것이 좋습니다. 읽기가 끝나면 약관을 읽었고 이에 동의함을 선택한 다음 약관 수락 및 보고서 다운로드를 선택합니다.
7. PDF 뷰어를 통해 다운로드한 파일을 엽니다. 동의 약관을 검토하고 아래로 스크롤하여 감사 보고서를 찾으십시오. 보고서에는 추가 정보가 PDF 문서 내에 첨부 파일로 포함될 수 있으므로 파일 내에 첨부 파일이 있는지 PDF 증빙 문서를 확인해야 합니다. 첨부 파일을 보는 방법에 대한 지침은 섹션을 참조하세요PDF 문서에서 첨부 파일 보기.

# PDF 문서에서 첨부 파일 보기

현재 PDF 첨부 파일 보기를 지원하는 다음 애플리케이션을 사용하는 것이 좋습니다.

Adobe Acrobat Reader

Adobe 웹 사이트 에서 최신 버전의 Adobe Acrobat Reader를 다운로드합니다https://get.adobe.com/reader/.

Acrobat Reader에서 PDF 첨부 파일을 보는 방법에 대한 지침은 Adobe Support 웹 사이트의 에서 링크 및 첨부 파일을 PDFs 참조하세요.

Firefox 브라우저

1. Mozilla 웹 사이트 https://www.mozilla.org/en-US/firefox/new 최신 Firefox 웹 브라우저를 다운로드합니다.
2. Firefox의 기본 제공 PDF 뷰어에서 PDF 파일을 엽니다. 지침은 Firefox에서 PDF 파일 보기를 참조하거나 Mozilla Support 웹 사이트에서 다른 뷰어를 선택합니다.
3. Firefox의 기본 제공 PDF 뷰어에서 PDF 첨부 파일을 보려면 사이드바 토글 , 첨부 파일 표시 를 선택합니다.

# 문서 보안 유지

AWS Artifact 문서는 기밀이며 항상 안전하게 보관해야 합니다. 는 문서에 대한 AWS 공동 책임 모델을 AWS Artifact 사용합니다. 즉, AWS 는 문서가 AWS 클라우드에 있는 동안 안전하게 유지할 책임이 있

지만 문서를 다운로드한 후에는 안전하게 유지할 책임이 있습니다. 문서를 다운로드 AWS Artifact 하기 전에 약관에 동의해야 할 수 있습니다. 각 문서 다운로드에는 추적 가능한 고유의 워터마크가 찍혀 있습니다.

기밀 표시가 된 문서는 회사 내부, 규제 당국, 감사 기관에만 공유할 수 있습니다. 고객과 혹은 자사 웹 사이트에 올려서 이런 문서를 공유하면 안 됩니다. Amazon 과 같은 보안 문서 공유 서비스를 사용하여 다른 사용자와 문서를 공유하는 WorkDocs것이 좋습니다. 이메일을 통해 문서를 보내거나 안전하지 않은 사이트에 업로드하지 마십시오.

# 문제 해결

문서를 다운로드하거나 오류 메시지를 받을 수 없는 경우 의 문제 해결을 참조하세요 AWS Artifact FAQ.

# 에서 계약 관리 AWS Artifact

AWS Artifact 를 사용하여 AWS 계정 또는 조직의 계약을 검토하고 관리할 수 있습니다. 예를 들어, 건강보험 이전 및 책임에 관한 법률(HIPAA)의 적용을 받는 회사는 일반적으로 보호 대상 건강 정보(BAA)가 적절하게 보호되도록 AWS 하기 위해와 비즈니스 제휴자 부록(PHI) 계약을 체결해야 합니다. AWS Artifact 콘솔에서 이러한 계약을 검토하고 수락할 수 있으며를 합법적으로 처리할 수 AWS 계정 있는를 지정할 수 있습니다PHI.

를 사용하는 경우 조직의 모든 사용자를 AWS대신하여 BAA와 같은 계약을 수락 AWS Organizations 할 수 AWS 계정 있습니다. 기존 및 후속 멤버 계정은 모두 자동으로 계약의 적용을 받으며를 합법적으로 처리할 수 있습니다PHI.

또한 AWS Artifact 를 사용하여 AWS 계정 사용자 또는 조직이 계약을 수락했는지 확인하고, 수락된 계약의 조건을 검토하여 의무를 이해할 수 있습니다. 계정 또는 조직이 더 이상 수락된 계약을 사용할 필요가 없는 경우를 사용하여 계약을 AWS Artifact 해지할 수 있습니다. 계약을 해지했지만 나중에 필요할 경우 계약을 다시 활성화할 수 있습니다.

내용

- AWS 계정 에서에 대한 계약 수락 AWS Artifact
- AWS 계정 에서에 대한 계약 종료 AWS Artifact
- 에서 조직에 대한 계약 수락 AWS Artifact
- 에서 조직에 대한 계약 종료 AWS Artifact
- 의 오프라인 계약 AWS Artifact

## AWS 계정 에서에 대한 계약 수락 AWS Artifact

AWS Artifact 콘솔을 사용하여에 AWS 대한 와의 계약을 검토하고 수락할 수 있습니다 AWS 계정.

> **Important**
>
> 계약을 수락하기 전에 귀사의 법무, 개인정보 보호, 규정 준수 팀과 협의할 것을 권장합니다.

필수 권한

계정의 관리자인 경우 IAM 사용자 및 페더레이션 사용자에게 하나 이상의 계약에 액세스하고 관리할 수 있는 권한을 부여할 수 있습니다. 기본적으로 관리자 권한이 있는 사용자만 계약을 수락할 수 있습니다. 계약을 수락하려면 IAM 페더레이션 사용자에게 필요한 권한이 있어야 합니다.

자세한 내용은 의 자격 증명 및 액세스 관리 AWS Artifact 단원을 참조하십시오.

와 계약을 수락하려면 AWS

1. 에서 AWS Artifact 콘솔을 엽니다https://console.aws.amazon.com/artifact/.
2. AWS Artifact 탐색 창에서 계약을 선택합니다.
3. 계정 계약 탭을 선택합니다.
4. 에서 AWS Artifact 콘솔을 엽니다https://console.aws.amazon.com/artifact/.
5. 탐색 창에서 계약을 선택합니다.
6. 계약 페이지에서 다음 중 하나를 수행합니다.
   - 계정에 대한 계약만 수락하려면 계정 계약 탭을 선택합니다.
   - 조직을 대신하여 계약을 수락하려면 조직 계약 탭을 선택합니다.
7. 계약을 선택한 다음 계약 다운로드를 선택합니다.

   보고서 NDA 다운로드 수락 대화 상자가 나타납니다.
8. 선택한 계약을 다운로드하려면 먼저 비공개 계약()의 AWS Artifact 약관에 동의해야 합니다AWS Artifact NDA.

   a. 보고서 NDA 다운로드 수락 대화 상자에서를 검토합니다 AWS Artifact NDA.

   b. (선택 사항) AWS Artifact NDA의 사본을 인쇄하려면(또는 로 저장하려면PDF) 인쇄NDA를 선택합니다.

   c. 의 모든 약관을 읽었으며 이에 동의합니다를 선택합니다NDA.

   d. 선택한 계약의 및를 AWS Artifact NDA 수락하고 다운로드하려면 수락 NDA 및 다운로드PDF를 선택합니다.
9. PDF 뷰어에서 다운로드PDF한 계약을 검토합니다.
10. AWS Artifact 콘솔에서 계약을 선택한 상태에서 계약 수락을 선택합니다.
11. 계약 수락 대화 상자에서 다음을 수행합니다.

    a. 계약을 검토합니다.

    b. 이 모든 이용 약관에 동의함을 선택합니다.

    c. 계약 수락을 선택합니다.

12. 본인 계정에 해당하는 계약을 수락하려면 적용을 선택합니다.

## AWS 계정 에서에 대한 계약 종료 AWS Artifact

AWS Artifact 콘솔을 사용하여 단일에 대한 계약을 수락 AWS 계정한 경우 콘솔을 사용하여 해당 계약을 해지할 수 있습니다. 그렇지 않으면 의 오프라인 계약 AWS Artifact 을 참조하십시오.

필수 권한

계약을 종료하려면 IAM 페더레이션 사용자에게 필요한 권한이 있어야 합니다.

자세한 내용은 의 자격 증명 및 액세스 관리 AWS Artifact 단원을 참조하십시오.

와의 온라인 계약을 해지하려면 AWS

1. 에서 AWS Artifact 콘솔을 엽니다https://console.aws.amazon.com/artifact/.
2. AWS Artifact 탐색 창에서 계약을 선택합니다.
3. 계정 계약 탭을 선택합니다.
4. 계약을 선택하고 계약 종료를 선택합니다.
5. 모든 확인란을 선택하여 계약 해지에 동의함을 나타냅니다.
6. 종료를 선택합니다. 확인 메시지가 나타나면 종료를 선택합니다.

## 에서 조직에 대한 계약 수락 AWS Artifact

AWS Organizations 조직의 관리 계정 소유자인 경우 조직의 모든 사용자를 AWS 대신하여와 계약을 수락할 수 AWS 계정 있습니다.

> **Important**
>
> 계약을 수락하기 전에 귀사의 법무, 개인정보 보호, 규정 준수 팀과 협의할 것을 권장합니다.

AWS Organizations 에는 통합 결제 기능과 모든 기능의 두 가지 기능 세트가 있습니다. 조직에 AWS Artifact 를 사용하려면 모든 기능에 대해 소속된 조직을 활성화해야 합니다. 조직에 통합 결제만 구성된 경우 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하십시오.

조직 계약을 수락하거나 종료하려면 올바른 AWS Artifact 권한으로 관리 계정에 로그인해야 합니다. `organizations:DescribeOrganization` 권한이 있는 멤버 계정의 사용자는 자신을 대신하여 수락된 조직 계약을 볼 수 있습니다.

자세한 내용은 AWS Organizations 사용 설명서의를 사용하여 조직의 계정 관리를 AWS Organizations 참조하세요.

필수 권한

계약을 수락하려면 관리 계정 소유자에게 필요한 권한이 있어야 합니다.

자세한 내용은 의 자격 증명 및 액세스 관리 AWS Artifact 단원을 참조하십시오.

조직에 대한 계약을 수락하려면

1. 에서 AWS Artifact 콘솔을 엽니다https://console.aws.amazon.com/artifact/.
2. AWS Artifact 대시보드에서 계약을 선택합니다.
3. 조직 계약 탭을 선택합니다.
4. 에서 AWS Artifact 콘솔을 엽니다https://console.aws.amazon.com/artifact/.
5. 탐색 창에서 계약을 선택합니다.
6. 계약 페이지에서 다음 중 하나를 수행합니다.
   - 계정에 대한 계약만 수락하려면 계정 계약 탭을 선택합니다.
   - 조직을 대신하여 계약을 수락하려면 조직 계약 탭을 선택합니다.
7. 계약을 선택한 다음 계약 다운로드를 선택합니다.

   보고서 NDA 다운로드 수락 대화 상자가 나타납니다.
8. 선택한 계약을 다운로드하려면 먼저 비공개 계약()의 AWS Artifact 약관에 동의해야 합니다AWS Artifact NDA.

   a. 보고서 NDA 다운로드 수락 대화 상자에서를 검토합니다 AWS Artifact NDA.

   b. (선택 사항) AWS Artifact NDA의 사본을 인쇄하려면(또는 로 저장하려면PDF) 인쇄NDA를 선택합니다.

   c. 의 모든 약관을 읽었으며 이에 동의합니다를 선택합니다NDA.

   d. 선택한 계약의 및를 AWS Artifact NDA 수락하고 다운로드하려면 수락 NDA 및 다운로드PDF를 선택합니다.
9. PDF 뷰어에서 다운로드PDF한 계약을 검토합니다.

10. AWS Artifact 콘솔에서 계약을 선택한 상태에서 계약 수락을 선택합니다.
11. 계약 수락 대화 상자에서 다음을 수행합니다.
    a. 계약을 검토합니다.
    b. 모든 이용 약관에 동의함을 선택합니다.
    c. 계약 수락을 선택합니다.
12. 조직의 모든 기존 및 향후 계정에 대한 계약을 수락하려면 수락을 선택합니다.

# 에서 조직에 대한 계약 종료 AWS Artifact

AWS Artifact 콘솔을 사용하여 조직의 모든 멤버 계정을 대신하여 계약을 수락 AWS Organizations한 경우 콘솔을 사용하여 해당 계약을 해지할 수 있습니다. 그렇지 않으면 의 오프라인 계약 AWS Artifact 단원을 참조하세요.

멤버 계정이 조직에서 제거되면 해당 멤버 계정에는 조직 계약이 더 오래 적용됩니다. 조직에서 멤버 계정을 제거하기 전에 관리 계정 관리자는 필요한 경우 새 계약을 체결할 수 있도록 이를 멤버 계정에 전달해야 합니다. AWS Artifact 콘솔의 계약 페이지의 조직 계약에서 활성 조직 계약 목록을 볼 수 있습니다.

에 대한 자세한 내용은 AWS Organizations 사용 설명서의를 사용하여 조직의 계정 관리를 AWS Organizations AWS Organizations참조하세요.

필수 권한

계약을 해지하려면 관리 계정 소유자에게 필요한 권한이 있어야 합니다.

자세한 내용은 의 자격 증명 및 액세스 관리 AWS Artifact 단원을 참조하십시오.

와의 온라인 조직 계약을 해지하려면 AWS

1. 에서 AWS Artifact 콘솔을 엽니다https://console.aws.amazon.com/artifact/.
2. AWS Artifact 대시보드에서 계약을 선택합니다.
3. 조직 계약 탭을 선택합니다.
4. 계약을 선택하고 계약 종료를 선택합니다.
5. 모든 확인란을 선택하여 계약 해지에 동의함을 나타냅니다.
6. 종료를 선택합니다. 확인 메시지가 나타나면 종료를 선택합니다.

# 의 오프라인 계약 AWS Artifact

기존 오프라인 계약이 있는 경우는 오프라인으로 수락한 계약을 AWS Artifact 표시합니다. 예를 들어 콘솔에 오프라인 비즈니스 관계자 부록(BAA)이 활성 상태로 표시될 수 있습니다. 활성화 상태란 계약이 수락되었다는 의미입니다. 오프라인 계약을 종료하려면 계약에 포함된 종료 지침 및 설명을 확인하십시오.

계정이 AWS Organizations 조직의 관리 계정인 경우 AWS Artifact 를 사용하여 조직의 모든 계정에 오프라인 계약 조건을 적용할 수 있습니다. 오프라인으로 수락한 계약을 조직 및 조직의 모든 계정에 적용하려면 필요한 권한이 있어야 합니다.

계정이 조직의 멤버 계정인 경우 오프라인 조직 계약을 볼 수 있는 권한이 있어야 합니다.

자세한 내용은 의 자격 증명 및 액세스 관리 AWS Artifact 단원을 참조하십시오.

# 에서 이메일 알림 구성 AWS Artifact

AWS Artifact 콘솔을 사용하여 의 계약 및 보고서에 대한 업데이트에 대한 이메일 알림을 구성할 수 있습니다 AWS Artifact. 는 를 사용하여 이러한 이메일 알림을 AWS Artifact 보냅니다 AWS 사용자 알림. 이메일 알림을 받으려면 AWS Artifact 먼저 사용자 알림 콘솔에서 AWS 사용자 알림 알림 허브를 선택해야 합니다. 그런 다음 AWS Artifact 콘솔에서 알림 수신자와 수신 알림을 지정하는 알림 설정에 대한 구성을 생성할 수 있습니다.

AWS Artifact 이메일 알림을 구성하려면 AWS Artifact 및 에 필요한 권한이 있어야 합니다 AWS 사용자 알림. 자세한 내용은 의 자격 증명 및 액세스 관리 AWS Artifact 단원을 참조하십시오.

내용



## 사전 조건: 에서 알림 허브 선택 사용자 알림

AWS Artifact 이메일 알림을 받으려면 먼저 사용자 알림 콘솔을 열고 데이터를 저장할 AWS 리전 에서 알림 허브를 선택해야 합니다 사용자 알림 . 가 알림을 보내는 데 AWS 사용자 알림 AWS Artifact 사용하는 에는 알림 허브를 선택해야 합니다.

알림 허브를 선택하려면

1. AWS 사용자 알림 콘솔의 알림 허브 페이지를 엽니다.
2. AWS 사용자 알림 리소스를 저장할 에서 알림 허브 AWS 리전 를 선택합니다. 기본적으로 사용자 알림 데이터는 미국 동부(버지니아 북부) 리전에 저장됩니다. 는 선택한 다른 리전에서 알림 데이터를 사용자 알림 복제합니다. 자세한 내용은 AWS 사용자 알림 사용 설명서의 알림 허브 설명서를 참조하세요.
3. [Save and continue]를 선택합니다.

# AWS Artifact 알림 설정에 대한 구성 생성

사용자 알림 알림 허브 를 선택한 후 AWS Artifact 콘솔에서 알림 설정에 대한 구성을 생성할 수 있습니다. 생성하는 구성에서 AWS Artifact 알림을 수신할 수신자 이메일 주소를 지정합니다. 또한 AWS Artifact 계약에 대한 업데이트, 모든 (또는 하위 집합) AWS Artifact 보고서에 대한 업데이트 등 이러한 수신자가 알림을 받을 업데이트도 지정합니다.

구성 생성

1. AWS Artifact 콘솔의 알림 설정 페이지를 엽니다.
2. 구성 생성을 선택합니다.
3. 구성 생성 페이지에서 다음을 수행합니다.
   - 계약에 대한 알림을 받으려면 계약에서 AWS 계약 업데이트를 선택한 상태로 유지합니다.
   - 보고서에 대한 알림을 받으려면 보고서 에서 AWS 보고서 업데이트를 선택한 상태로 유지합니다.

     a. 모든 보고서에 대한 알림을 받으려면 모든 보고서 를 선택합니다.

     b. 특정 범주 및 시리즈의 보고서에 대한 알림만 받으려면 보고서 하위 집합을 선택합니다. 그런 다음 관심 있는 범주와 시리즈를 선택합니다.
   - 구성 이름 에 구성의 이름을 입력합니다.
   - 이메일 의 수신자 에 AWS Artifact 알림 이메일을 수신할 이메일 주소 목록을 쉼표로 구분하여 입력합니다.
   - (선택 사항) 알림 구성에 태그를 추가하려면 태그 를 확장하고 새 태그 추가 를 선택한 다음 키-값 페어로 태그를 입력합니다. 사용자 알림 리소스 태그 지정에 대한 자세한 내용은 AWS 사용자 알림 사용 설명서의 AWS 사용자 알림 리소스 태그 지정을 참조하세요.
   - 구성 생성을 선택합니다.

     사용자 알림 는 사용자가 제공한 각 수신자 이메일 주소로 확인 이메일을 보냅니다. 이메일 주소를 확인하려면 확인 이메일에서 수신자가 이메일 확인을 선택해야 합니다. 확인된 이메일 주소만 AWS Artifact 알림을 수신합니다.

# AWS Artifact 알림 설정에 대한 구성 편집

AWS Artifact 알림 설정에 대한 구성을 생성한 후 언제든지 구성을 편집하여 알림 설정을 변경할 수 있습니다. 예를 들어 수신자를 추가하거나 제거하려면 수신자가 수신하는 알림 유형을 변경하고 태그를 추가하거나 제거합니다.

구성을 편집하려면

1. AWS Artifact 콘솔의 알림 설정 페이지를 엽니다.
2. 편집하려는 구성을 선택합니다.
3. 편집을 선택합니다.
4. 구성 선택 및 필드를 편집합니다. 완료되면 변경 사항 저장을 선택합니다.

   새 이메일 주소를 알림 수신자로 추가한 경우 는 해당 이메일 주소를 확인 이메일로 AWS 사용자 알림 보냅니다. 이메일 주소를 확인하려면 확인 이메일에서 수신자가 이메일 확인을 선택해야 합니다. 확인된 이메일 주소만 AWS Artifact 알림을 수신합니다.

# AWS Artifact 알림 설정에 대한 구성 삭제

AWS Artifact 알림 설정을 위해 생성한 구성이 더 이상 필요하지 않은 경우 AWS Artifact 콘솔에서 구성을 삭제할 수 있습니다.

구성을 삭제하려면

1. AWS Artifact 콘솔의 알림 설정 페이지를 엽니다.
2. 삭제할 구성을 선택합니다.
3. Delete(삭제)를 선택합니다.
4. 구성 삭제 대화 상자에서 삭제를 선택합니다.

# 의 자격 증명 및 액세스 관리 AWS Artifact

가입할 때 AWS 계정과 연결된 이메일 주소와 암호를 AWS제공합니다. 이는 루트 자격 증명이며에 대한 AWS 리소스를 포함한 모든 리소스에 대한 완전한 액세스를 제공합니다 AWS Artifact. 그러나 일상적인 액세스에는 루트 계정을 사용하지 않을 것을 강력 권장합니다. 또한 계정 자격 증명을 다른 사람과 공유하여 내 계정에 대한 전체 액세스 권한을 주는 것도 피하도록 합니다.

루트 자격 증명으로 AWS 계정에 로그인하거나 자격 증명을 다른 사용자와 공유하는 대신, 사용자 본인과 문서 또는 계약에 액세스해야 할 수 있는 모든 사람을 위해 IAM 사용자라는 특수 사용자 자격 증명을 생성해야 합니다 AWS Artifact. 이렇게 하면 각 사용자에게 개별 로그인 정보를 제공하여 특정 문서를 사용하는 데 필요한 권한만 사용자별로 부여할 수 있습니다. IAM 그룹에 권한을 부여하고 IAM 사용자를 추가하면 여러 IAM 사용자에게 동일한 권한을 부여할 수 있습니다.

외부에서 사용자 ID를 이미 관리하는 경우 IAM 사용자를 생성하는 대신 IAM ID 공급자를 사용할 AWS 수 있습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자 및 연동을 참조하세요.

내용

- 에 대한 사용자 액세스 권한 부여 AWS Artifact
- 에 대한 세분화된 권한으로 보고서 마이그레이션 AWS Artifact
- AWS Artifact 계약에 대한 세분화된 권한으로 마이그레이션
- 에 대한 IAM 정책 예제 AWS Artifact
- 에 대한 AWS 관리형 정책 사용 AWS Artifact
- AWS Artifact에 서비스 연결 역할 사용
- AWS Artifact 보고서에 IAM 조건 키 사용

## 에 대한 사용자 액세스 권한 부여 AWS Artifact

다음 단계를 완료하여 사용자에게 필요한 액세스 수준에 AWS Artifact 따라 에 권한을 부여합니다.

Tasks

- 1단계: IAM 정책 생성
- 2단계: IAM 그룹 생성 및 정책 연결
- 3단계: IAM 사용자 생성 및 그룹에 추가

## 1단계: IAM 정책 생성

IAM 관리자는 AWS Artifact 작업 및 리소스에 권한을 부여하는 정책을 생성할 수 있습니다.

IAM 정책 생성

다음 절차에 따라 IAM 사용자 및 그룹에 권한을 부여하는 데 사용할 수 있는 IAM 정책을 생성합니다.

1. 에서 IAM 콘솔을 엽니다https://console.aws.amazon.com/iam/.
2. 탐색 창에서 Policies를 선택합니다.
3. 정책 생성을 선택합니다.
4. JSON 탭을 선택합니다.
5. 정책 문서를 입력합니다. 정책을 직접 생성하거나 에 대한 IAM 정책 예제 AWS Artifact의 정책 중 하나를 사용할 수 있습니다.
6. 정책 검토를 선택합니다. 정책 검사기가 모든 구문 오류를 보고합니다.
7. 정책 검토 페이지에서 정책의 목적을 기억하는 데 도움이 되는 고유한 이름을 입력합니다. 설명을 추가할 수도 있습니다.
8. 정책 생성을 선택합니다.

## 2단계: IAM 그룹 생성 및 정책 연결

IAM 관리자는 그룹을 생성하고 생성한 정책을 그룹에 연결할 수 있습니다. 언제든지 그룹에 IAM 사용자를 추가할 수 있습니다.

IAM 그룹을 생성하고 정책을 연결하려면

1. 탐색 창에서 그룹을 선택한 다음, 새 그룹 생성을 선택합니다.
2. 그룹 이름에서 그룹 이름을 입력한 다음, 다음 단계를 선택합니다.
3. 생성한 정책 이름을 검색 창에 입력합니다. 정책의 확인란을 선택한 후 다음 단계를 선택합니다.
4. 그룹 이름 및 정책을 검토합니다. 준비가 됐으면 그룹 생성을 선택합니다.

## 3단계: IAM 사용자 생성 및 그룹에 추가

IAM 관리자는 언제든지 그룹에 사용자를 추가할 수 있습니다. 그러면 그룹에 부여된 권한이 사용자에게 부여됩니다.

IAM 사용자를 생성하고 그룹에 추가하려면

1. 탐색 창에서 사용자와 사용자 추가를 차례로 선택합니다.
2. 사용자 이름에는 한 명 이상의 사용자 이름을 입력합니다.
3. AWS Management Console 액세스 옆의 확인란을 선택합니다. 자동 생성 암호 또는 사용자 지정 암호를 구성합니다. 다음 로그인 시 사용자가 새 암호를 생성해야 함을 선택하여 사용자가 처음 로그인할 때 암호를 재설정하도록 요구할 수 있습니다.
4. 다음: 권한을 선택합니다.
5. 그룹에 사용자 추가를 선택한 다음 생성한 그룹을 선택합니다.
6. 다음: 태그를 선택합니다. 사용자에게 태그를 추가할 수 있습니다.
7. 다음: 검토를 선택합니다. 준비가 됐으면 사용자 생성을 선택합니다.

# 에 대한 세분화된 권한으로 보고서 마이그레이션 AWS Artifact

이제에 대해 세분화된 권한을 사용할 수 있습니다 AWS Artifact. 이러한 세분화된 권한을 통해 용어 수락 및 보고서 다운로드와 같은 기능에 대한 액세스를 제공하는 것을 세부적으로 제어할 수 있습니다.

세분화된 권한을 통해 보고서에 액세스하려면 아래 권장 사항에 따라 AWSArtifactReportsReadOnlyAccess 관리형 정책을 활용하거나 권한을 업데이트할 수 있습니다. 이전에 세분화된 권한 사용을 옵트아웃한 경우 보고서 콘솔에서 사용할 수 있는 “AWS아티팩트 보고서에 대한 세분화된 권한에 대한 옵트인” 링크를 사용하여 옵트인해야 합니다.

새 권한을 업데이트하는 데 문제가 있는 경우 콘솔에서 사용할 수 있는 “AWS아티팩트 보고서에 대한 세분화된 권한 옵트아웃” 링크를 통해 이전 권한이 있는 보고서에 액세스할 수 있습니다.

## 보고서를 새 권한으로 마이그레이션

리소스가 아닌 특정 권한 마이그레이션

레거시 권한이 포함된 기존 정책을 세분화된 권한이 포함된 정책으로 바꿉니다.

레거시 정책:

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

```
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
            "arn:aws:artifact:::report-package/*"
        ]
    }]
}
```

세분화된 권한이 있는 새 정책:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:ListReports",
            "artifact:GetReportMetadata",
            "artifact:GetReport",
            "artifact:GetTermForReport"
        ],
        "Resource": "*"
    }]
}
```

특정 리소스 권한 마이그레이션

레거시 권한이 포함된 기존 정책을 세분화된 권한이 포함된 정책으로 바꿉니다. 보고서 리소스 와일드카드 권한이 조건 키로 대체되었습니다.

레거시 정책:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
```

```
        "Resource": [
            "arn:aws:artifact:::report-package/Certifications and Attestations/SOC/*",
            "arn:aws:artifact:::report-package/Certifications and Attestations/PCI/*",
            "arn:aws:artifact:::report-package/Certifications and Attestations/ISO/*"
        ]
    }]
}
```

세분화된 권한 및 조건 키가 포함된 새 정책:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "artifact:GetReportMetadata",
                "artifact:GetReport",
                "artifact:GetTermForReport"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": [
                        "SOC",
                        "PCI",
                        "ISO"
                    ],
                    "artifact:ReportCategory": [
                        "Certifications and Attestations"
                    ]
                }
            }
        }
    ]
}
```

# AWS Artifact 계약에 대한 세분화된 권한으로 마이그레이션

AWS 이제 아티팩트를 통해 고객은 계약에 세분화된 권한을 사용할 수 있습니다. 이러한 세분화된 권한을 통해 고객은 비공개 계약 확인 및 수락, 계약 수락 및 해지와 같은 기능에 대한 액세스 권한을 세부적으로 제어할 수 있습니다.

세분화된 권한을 통해 계약에 액세스하려면 AWSArtifactAgreementsReadOnlyAccess 또는 AWSArtifactAgreementsFullAccess 관리형 정책을 활용하거나 아래 권장 사항에 따라 권한을 업데이트할 수 있습니다. 이전에 세분화된 권한 사용을 옵트아웃한 경우 계약 콘솔에서 사용할 수 있는 “AWS아티팩트 계약에 대한 세분화된 권한에 대한 옵트인” 링크를 사용하여 옵트인해야 합니다.

새 권한을 업데이트하는 데 문제가 있는 경우 콘솔에서 사용할 수 있는 “AWS아티팩트 계약에 대한 세분화된 권한 옵트아웃” 링크를 통해 이전 권한이 있는 계약에 액세스할 수 있습니다.

## 새 권한으로 마이그레이션

레거시 IAM 작업 "DownloadAgreement"이 수락되지 않은 계약을 다운로드하는 "GetAgreement" 작업과 수락된 계약을 다운로드하는 "GetCustomerAgreement" 작업으로 대체되었습니다. 또한 비공개 계약()을 보고 수락하기 위한 액세스를 제어하기 위해 보다 세분화된 작업이 도입되었습니다NDAs. 이러한 세분화된 작업을 활용하고 계약을 보고 실행할 수 있는 기능을 유지하려면 사용자는 레거시 권한이 포함된 기존 정책을 세분화된 권한이 포함된 정책으로 바꿔야 합니다.

권한을 마이그레이션하여 계정 수준에서 계약 다운로드

기존 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
```

```
}
```

세분화된 권한이 포함된 새 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:GetAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptNdaForAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

리소스가 아닌 특정 권한을 마이그레이션하여 계정 수준에서 계약을 다운로드, 수락 및 종료

기존 정책:

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

```
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

세분화된 권한이 포함된 새 정책:

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
        "Sid": "ListAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:ListAgreements",
            "artifact:ListCustomerAgreements"
        ],
        "Resource": "*"
      },
      {
        "Sid": "AWSAgreementActions",
        "Effect": "Allow",
        "Action": [
          "artifact:GetAgreement",
          "artifact:AcceptNdaForAgreement",
          "artifact:GetNdaForAgreement",
          "artifact:AcceptAgreement"
        ],
        "Resource": "arn:aws:artifact:::agreement/*"
      },
      {
        "Sid": "CustomerAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:GetCustomerAgreement",
```

```
            "artifact:TerminateAgreement"
        ],
        "Resource": "arn:aws:artifact::*:customer-agreement/*"
      }
    ]
}
```

리소스가 아닌 특정 권한을 마이그레이션하여 조직 수준에서 계약을 다운로드, 수락 및 종료합니다.

기존 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam:::role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam:::role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
```

```
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

세분화된 권한이 포함된 새 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
```

```
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

리소스별 권한을 마이그레이션하여 계정 수준에서 계약을 다운로드, 수락 및 종료

기존 정책:

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

```
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact:::agreement/AWS Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*"
      ]
    }
  ]
}
```

세분화된 권한이 포함된 새 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
```

```
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

리소스별 권한을 마이그레이션하여 조직 수준에서 계약을 다운로드, 수락 및 종료합니다.

기존 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/AWS Organizations Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam:::role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
```

```
      "Resource": "arn:aws:iam:::role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

세분화된 권한이 포함된 새 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv"
    },
    {
      "Sid": "CustomerAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

## 계약에 대한 레거시에서 세분화된 리소스 매핑

세분화된 권한에 대해 ARN의 계약이 업데이트되었습니다. 레거시 계약 리소스에 대한 이전 참조는 새로 대체해야 합니다ARN. 다음은 레거시 리소스와 세분화된 리소스 간의 계약 ARN 매핑입니다.

| 계약 이름 | 레거시 권한ARN에 대한 아티팩트 | 세분화된 권한ARN에 대한 아티팩트 |
| --- | --- | --- |
| AWS 비즈니스 파트너 부록 | arn:aws:artifact:::agreement/AWS Business Associate 부록 | arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm |
| AWS 뉴질랜드 인증 데이터 위반 부록 | arn:aws:artifact:::agreement/AWS New Zealand Notifiable Data Breach Addendum | arn:aws:artifact:::agreement/agreement-3YRq9rGUIu72r7Gt |
| AWS 호주 인증 데이터 위반 부록 | arn:aws:artifact:::agreement/AWS Australian Notifiable Data Breach Addendum | arn:aws:artifact:::agreement/agreement-sbLSDe8bitmAXNr9 |
| AWS SEC 규칙 17a-4 부록 | arn:aws:artifact:::agreement/AWS SEC 규칙 17a-4 부록 | arn:aws:artifact:::agreement/agreement-bexgr7sjvXAW4Gxu |
| AWS SEC 규칙 18a-6 부록 | arn:aws:artifact:::agreement/AWS SEC 규칙 18a-6 부록 | arn:aws:artifact:::agreement/agreement-HZTdNwJuqOKLReXC |
| AWS Organizations Business Associate 부록 | arn:aws:artifact:::agreement/AWS Organizations Business Associate 부록 | arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv |
| AWS Organizations Australian Notifiable Data Breach 부록 | arn:aws:artifact::agreement/AWS Organizations Australian Notifiable Data Breach Addendum | arn:aws:artifact:::agreement/agreement-YpDMFXTePE7kEg4b |

| 계약 이름 | 레거시 권한ARN에 대한 아티팩트 | 세분화된 권한ARN에 대한 아티팩트 |
| --- | --- | --- |
| AWS Organizations New Zealand Notifiable Data Breach 부록 | arn:aws:artifact:::agreement/AWS Organizations New Zealand Notifiable Data Breach Addendum | arn:aws:artifact:::agreement/agreement-uojEjr3vOnvrhV52 |

# 에 대한 IAM 정책 예제 AWS Artifact

IAM 사용자에게 권한을 부여하는 권한 정책을 생성할 수 있습니다. 사용자에게 AWS Artifact 보고서에 대한 액세스 권한과 단일 계정 또는 조직을 대신하여 계약을 수락하고 다운로드할 수 있는 권한을 부여할 수 있습니다.

다음 예제 정책은 필요한 액세스 수준에 따라 IAM 사용자에게 할당할 수 있는 권한을 보여줍니다.

- 세분화된 권한으로 AWS 보고서를 관리하는 정책 예제
- 타사 보고서를 관리하기 위한 정책 예시
- 계약 관리 정책 예시
- 와 통합할 정책 예제 AWS Organizations
- 관리 계정의 계약을 관리하기 위한 정책 예시
- 조직 계약을 관리하기 위한 정책 예시
- 알림 관리를 위한 정책 예시

Example 세분화된 권한을 통해 AWS 보고서를 관리하는 정책 예제

> **Tip**
>
> 자체 AWSArtifactReportsReadOnlyAccess 정책을 정의하는 대신 관리형 정책을 사용하는 것이 좋습니다.

다음 정책은 세분화된 권한을 통해 모든 AWS 보고서를 다운로드할 수 있는 권한을 부여합니다.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

다음 정책은 세분화된 권한을 통해 AWS SOC, PCI및 ISO 보고서만 다운로드할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications And Attestations"
          ]
        }
      }
    }
```

```
  ]
}
```

Example 타사 보고서를 관리하기 위한 정책 예시

> **Tip**
>
> 자체 AWSArtifactReportsReadOnlyAccess 정책을 정의하는 대신 관리형 정책을 사용하는 것이 좋습니다.

타사 보고서는 IAM 리소스 로 표시됩니다`report`.

다음 정책은 모든 타사 보고서 기능에 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

다음 정책은 타사 보고서를 다운로드할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

다음 정책은 타사 보고서를 열거할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReport"
      ],
      "Resource": "*"
    }
  ]
}
```

다음 정책은 모든 버전에 대한 타사 보고서의 세부 정보를 볼 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

다음 정책은 특정 버전에 대한 타사 보고서의 세부 정보를 볼 수 있는 권한을 부여합니다.

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:1"
      ]
    }
  ]
}
```

> **Tip**
>
> 자체 AWSArtifactAgreementsReadOnlyAccess 정책을 정의하는 대신 또는 AWSArtifactAgreementsFullAccess 관리형 정책을 사용하는 것이 좋습니다.

Example 계약 관리 정책 예시

다음 정책은 모든 계약을 다운로드할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
```

```
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

다음 정책은 모든 계약을 수락할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
}
```

다음 정책은 모든 계약을 종료할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

다음 정책은 계정 수준 계약을 보고 실행할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
```

```
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

### Example 와 통합할 정책 예제 AWS Organizations

다음 정책은가와 통합하는 데 AWS Artifact 사용하는 IAM 역할을 생성할 수 있는 권한을 부여합니다 AWS Organizations. 조직의 관리 계정은 이들 권한이 있어야 조직 계약을 시작할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

다음 정책은 사용 권한을 부여할 수 AWS Artifact 있는 권한을 부여합니다 AWS Organizations. 조직의 관리 계정은 이들 권한이 있어야 조직 계약을 시작할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
   }
 ]
}
```

Example 관리 계정의 계약을 관리하기 위한 정책 예시

다음 정책은 관리 계정의 계약을 관리할 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
```

```
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

Example 조직 계약을 관리하기 위한 정책 예시

다음 정책은 조직 계약을 관리할 권한을 부여합니다. 필요한 권한이 있는 다른 사용자가 조직 계약을 설정해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

다음 정책은 조직 계약을 볼 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 알림 관리를 위한 정책 예시

다음 정책은 AWS Artifact 알림을 사용할 수 있는 전체 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:DeleteEmailContact",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:SendActivationCode"
```

```
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

다음 정책은 모든 구성을 열거할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

다음 정책은 구성을 생성할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:SendActivationCode",
        "notifications:AssociateChannel",
```

```
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:ListEventRules",
        "notifications:ListNotificationHubs",
        "notifications:TagResource",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

다음 정책은 구성을 편집할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

다음 정책은 구성을 삭제할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

다음 정책은 구성 세부 정보를 볼 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

다음 정책은 알림 허브를 등록 또는 등록 취소할 권한을 부여합니다.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

# 에 대한 AWS 관리형 정책 사용 AWS Artifact

AWS 관리형 정책은에서 생성 및 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 AWS 관리형 정책에 정의된 권한을 AWS 업데이트하면 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS 는 새 AWS 서비스 가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM사용 설명서의 AWS 관리형 정책을 참조하세요.

## AWS 관리형 정책: AWSArtifactReportsReadOnlyAccess

`AWSArtifactReportsReadOnlyAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 보고서 나열, 보기 및 다운로드를 허용하는 *read-only* 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `artifact` - 보안 주체가 보고서를 나열, 확인 및 다운로드할 수 있습니다 AWS Artifact.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

## AWS 관리형 정책: AWSArtifactAgreementsReadOnlyAccess

`AWSArtifactAgreementsReadOnlyAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 AWS Artifact 서비스 계약을 나열하고 수락된 계약을 다운로드할 수 있는 *read-only* 액세스 권한을 부여합니다. 또한 조직 세부 정보를 나열하고 설명할 수 있는 권한도 포함되어 있습니다. 또한 이 정책은 필요한 서비스 연결 역할이 존재하는지 확인할 수 있는 기능을 제공합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `artifact` - 보안 주체가 모든 계약을 나열하고 수락된 계약을 볼 수 있도록 허용합니다 AWS Artifact.

- IAM - 보안 주체가를 사용하여 서비스 연결 역할이 존재하는지 확인할 수 있습니다 GetRole.
- organization - 보안 주체가 조직을 설명하고 조직의 서비스 액세스를 나열할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetCustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "AWSOrganizationActions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
```

```
}
```

## AWS 관리형 정책: AWSArtifactAgreementsFullAccess

`AWSArtifactAgreementsFullAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 AWS 아티팩트 계약을 나열, 다운로드, 수락 및 종료할 수 있는 *`full`* 권한을 부여합니다. 또한 Organization 서비스에서 AWS 서비스 액세스를 나열 및 활성화하고 조직 세부 정보를 설명할 수 있는 권한도 포함되어 있습니다. 또한이 정책은 필요한 서비스 연결 역할이 존재하는지 확인하고 존재하지 않는 경우 이를 생성하는 기능을 제공합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `artifact` - 보안 주체가 계약을 나열, 다운로드, 수락 및 종료할 수 있습니다 AWS Artifact.
- `IAM` - 보안 주체가 서비스 연결 역할을 생성하고를 사용하여 서비스 연결 역할이 존재하는지 확인할 수 있습니다 GetRole.
- `organization` - 보안 주체가 조직을 설명하고 조직에 대한 서비스 액세스를 나열/활성화할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
```

```
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

## AWS ArtifactAWS 관리형 정책에 대한 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Artifact 이후에 대한 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Artifact 문서 기록 페이지에서 RSS 피드를 구독하세요.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWS Artifact 변경 사항 추적 시작 | AWS Artifact 는 AWS 관리형 정책에 대한 변경 사항을 추적하기 시작하여 도입했습니다 AWSArtifactReportsReadOnlyAccess. | 2023-12-15 |
| AWS 계약 관리형 정책 도입 | 정책 도입 AWSArtifactAgreementsReadOnlyAccess 및 AWSArtifactAgreementsFullAccess 관리. | 2024-11-21 |

# AWS Artifact에 서비스 연결 역할 사용

AWS Artifact 는 AWS Identity and Access Management (IAM) 서비스 연결 역할 을 사용합니다. 서비스 연결 역할은 에 직접 연결된 고유한 유형의 IAM 역할입니다 AWS Artifact. 서비스 연결 역할은 에서 사전 정의 AWS Artifact 하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할을 더 AWS Artifact 쉽게 설정할 수 있습니다. 는 서비스 연결 역할의 권한을 AWS Artifact 정의하며, 달리 정의되지 않는 한 만 역할을 수

임 AWS Artifact 할 수 있습니다. 정의된 권한에는 신뢰 정책 및 권한 정책이 포함되며 해당 권한 정책은 다른 IAM엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 AWS Artifact 리소스에 액세스할 수 있는 권한을 실수로 제거할 수 없기 때문에 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 서비스 연결 역할 열에서 AWS 로 작업하는 서비스를 IAM 참조하고 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

## 에 대한 서비스 연결 역할 권한 AWS Artifact

AWS Artifact 는 AWSServiceRoleForArtifact 라는 서비스 연결 역할을 사용합니다. 는 AWS Artifact 를 통해 조직에 대한 정보를 수집할 수 있습니다 AWS Organizations.

AWSServiceRoleForArtifact 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `artifact.amazonaws.com`

라는 역할 권한 정책은 AWS Artifact 가 `organizations` 리소스에서 다음 작업을 완료할 수 있도록 AWSArtifactServiceRolePolicy 허용합니다.

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

## 에 대한 서비스 연결 역할 생성 AWS Artifact

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 조직 관리 계정의 조직 계약 탭으로 이동하여 에서 시작하기 링크를 선택하면 서비스 연결 역할이 AWS Management Console AWS Artifact 생성됩니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 조직 관리 계정의 조직 계약 탭으로 이동하여 시작하기 링크를 선택하면 에서 서비스 연결 역할을 다시 AWS Artifact 생성합니다.

## 에 대한 서비스 연결 역할 편집 AWS Artifact

AWS Artifact 에서는 AWSServiceRoleForArtifact 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 를 사용하여 역할에 대한 설명을 편집할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

## 에 대한 서비스 연결 역할 삭제 AWS Artifact

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 이렇게 하면 적극적으로 모니터링하거나 유지 관리하지 않은 미사용 엔터티가 없습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스 삭제를 시도할 때 AWS Artifact 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

에서 사용하는 AWS Artifact 리소스를 삭제하려면 AWSServiceRoleForArtifact

1. AWS Artifact 콘솔의 '조직 계약' 테이블을 방문하세요.
2. 활성 조직 계약 종료

를 사용하여 서비스 연결 역할을 수동으로 삭제하려면 IAM

IAM 콘솔, AWS CLI또는 AWS API 를 사용하여 AWSServiceRoleForArtifact 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

## AWS Artifact 서비스 연결 역할에 지원되는 리전

AWS Artifact 는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원하지 않습니다. 다음 리전에서 AWSServiceRoleForArtifact 역할을 사용할 수 있습니다.

| 지역명 | 리전 자격 증명 | 에서 지원 AWS Artifact |
|---|---|---|
| 미국 동부(버지니아 북부) | us-east-1 | 예 |
| 미국 동부(오하이오) | us-east-2 | 아니요 |

| 지역명 | 리전 자격 증명 | 에서 지원 AWS Artifact |
|---|---|---|
| 미국 서부(캘리포니아 북부) | us-west-1 | 아니요 |
| 미국 서부(오레곤) | us-west-2 | 예 |
| 아프리카(케이프타운) | af-south-1 | 아니요 |
| 아시아 태평양(홍콩) | ap-east-1 | 아니요 |
| 아시아 태평양(자카르타) | ap-southeast-3 | 아니요 |
| 아시아 태평양(뭄바이) | ap-south-1 | 아니요 |
| 아시아 태평양(오사카) | ap-northeast-3 | 아니요 |
| 아시아 태평양(서울) | ap-northeast-2 | 아니요 |
| 아시아 태평양(싱가포르) | ap-southeast-1 | 아니요 |
| 아시아 태평양(시드니) | ap-southeast-2 | 아니요 |
| 아시아 태평양(도쿄) | ap-northeast-1 | 아니요 |
| 캐나다(중부) | ca-central-1 | 아니요 |
| 유럽(프랑크푸르트) | eu-central-1 | 아니요 |
| 유럽(아일랜드) | eu-west-1 | 아니요 |
| 유럽(런던) | eu-west-2 | 아니요 |
| 유럽(밀라노) | eu-south-1 | 아니요 |
| 유럽(파리) | eu-west-3 | 아니요 |
| 유럽(스톡홀름) | eu-north-1 | 아니요 |
| 중동(바레인) | me-south-1 | 아니요 |
| 중동(UAE) | me-central-1 | 아니요 |

| 지역명 | 리전 자격 증명 | 에서 지원 AWS Artifact |
|---|---|---|
| 남아메리카(상파울루) | sa-east-1 | 아니요 |
| AWS GovCloud (미국 동부) | us-gov-east-1 | 아니요 |
| AWS GovCloud (미국 서부) | us-gov-west-1 | 아니요 |

# AWS Artifact 보고서에 IAM 조건 키 사용

IAM 조건 키를 사용하여 특정 보고서 범주 및 시리즈에 AWS Artifact따라 의 보고서에 대한 세분화된 액세스를 제공할 수 있습니다.

다음 예제 정책은 특정 보고서 범주 및 시리즈를 기반으로 IAM 사용자에게 할당할 수 있는 권한을 보여줍니다.

Example AWS 보고서 읽기 액세스를 관리하기 위한 정책 예제

AWS Artifact 보고서는 IAM 리소스 로 표시됩니다`report`.

다음 정책은 `Certifications and Attestations` 범주의 모든 AWS Artifact 보고서를 읽을 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

다음 정책을 통해 SOC 시리즈의 모든 AWS Artifact 보고서를 읽을 수 있는 권한을 부여할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": [
                "artifact:GetReport",
                "artifact:GetReportMetadata",
                "artifact:GetTermForReport"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": "SOC",
                    "artifact:ReportCategory": "Certifications and Attestations"
                }
            }
        }
    ]
}
```

다음 정책을 통해 `Certifications and Attestations` 범주에 속하는 보고서를 제외한 모든 AWS Artifact 보고서를 읽을 수 있는 권한을 부여할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

# 를 사용하여 통화 로깅 AWS Artifact API AWS CloudTrail

AWS Artifact 는 사용자 AWS CloudTrail, 역할 또는 서비스 in AWS Artifact. CloudTrail Capture가를 이벤트 AWS Artifact 로 API 호출하는 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. 캡처된 호출에는 AWS Artifact 콘솔의 호출과 작업에 대한 코드 호출이 AWS Artifact API 포함됩니다. 추적을 생성하는 경우에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다 AWS Artifact. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. 에서 수집한 정보를 사용하여에 수행된 요청 CloudTrail, 요청이 수행된 AWS Artifact IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

자세한 내용은 AWS CloudTrail 사용 설명서를 CloudTrail참조하세요.

## AWS Artifact 의 정보 CloudTrail

CloudTrail 는 계정을 생성할 AWS 계정 때에서 활성화됩니다. 에서 활동이 발생하면 AWS Artifact해당 활동은 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록을 사용하여 CloudTrail 이벤트 보기를 참조하세요.

에 대한 이벤트를 AWS 계정포함하여에서 이벤트에 대한 지속적인 기록을 위해 추적을 AWS Artifact 생성합니다. 추적 CloudTrail 을 사용하면가 Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 사용자가 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

AWS Artifact 는 다음 작업을 CloudTrail 로그 파일에 이벤트로 로깅할 수 있도록 지원합니다.

- ListReports
- GetAccountSettings

- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings
- AcceptAgreement
- AcceptNdaForAgreement
- GetAgreement
- GetCustomerAgreement
- GetNdaForAgreement
- ListAgreements
- ListCustomerAgreements
- TerminateAgreement

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에서 이루어졌는지 여부입니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

## AWS Artifact 로그 파일 항목 이해

추적은 사용자가 지정한 Amazon S3 버킷으로 이벤트를 전송할 수 있도록 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함됩니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제에서는 GetReportMetadata 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "Records": [
```

```
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
 authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
```

```
        "reportId": "report-f1DIWBmGa2Lhsadg"
      },
      "responseElements": null,
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    }
  ]
}
```

# 에 대한 문서 기록 AWS Artifact

다음 표에서는 AWS Artifact 사용 설명서의 AWS Artifact 릴리스 및 관련 변경 사항 기록을 제공합니다.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 계약 실행 AWSArtifactAgreementsFullAccess 및 AWSArtifactAgreementsReadOnlyAccess 관리형 정책에 대한 세분화된 권한 | AWS Artifact 계약 실행 및 시작 AWSArtifactAgreementsFullAccess 및 AWSArtifactAgreementsReadOnlyAccess AWS 관리형 정책에 대한 세분화된 액세스를 활성화했습니다. | 2024년 11월 21일 |
| 세분화된 보고서 액세스 및 AWSArtifactReportReadOnlyAccess 관리형 정책 | AWS Artifact 보고서에 대한 세분화된 액세스를 활성화하고, 보고서 조건 키를 활성화하고, AWSArtifactReportsReadOnlyAccess 관리형 정책을 시작했습니다. | 2023년 12월 15일 |
| AWS Artifact 서비스 연결 역할 | 서비스 연결 역할 설명서를 추가하고 AWS Artifact 및 AWS Organizations 통합에 대한 예제 정책을 업데이트했습니다. | 2023년 9월 26일 |
| 알림 | 알림 관리를 위한 설명서를 게시하고 참조, CloudTrail 로깅 설명서 및 자격 증명 및 액세스 관리 페이지를 관련 AWS Artifact API 업데이트했습니다. | 2023년 8월 1일 |
| 타사 보고서 - 일반적으로 사용 가능 | API 참조 설명서 및 CloudTrail 로깅 설명서가 추가되었고 타사 보고서를 일반적으로 사용할 수 있게 되었습니다. | 2023년 1월 27일 |

| | | |
|---|---|---|
| 타사 보고서(미리 보기) | 제품을 판매하는 독립 소프트웨어 공급업체(ISVs)의 규정 준수 보고서를 시작했습니다 AWS Marketplace. 타사 보고서의 ID 및 액세스 관리 페이지에 정책 예제가 추가되었습니다. | 2022년 11월 30일 |
| 보안 | 혼동된 대리자 방지를 위해 자격 증명 및 액세스 관리 페이지에 섹션을 추가했습니다. | 2021년 12월 20일 |
| 보고서 | 비공개 계약을 제거하고 보고서 다운로드에 대한 이용 약관을 도입했습니다. | 2020년 12월 17일 |
| 홈페이지 및 검색 | 보고서 및 계약 페이지에 서비스 홈 페이지 및 검색 표시줄을 추가했습니다. | 2020년 5월 15일 |
| GovCloud 시작 | AWS Artifact 에서 시작되었습니다 AWS GovCloud (US) Regions. | 2019년 11월 7일 |
| AWS Organizations 계약 | 조직의 계약 관리에 대한 지원이 추가되었습니다. | 2018년 6월 20일 |
| 계약 | AWS Artifact 계약 관리에 대한 지원이 추가되었습니다. | 2017년 6월 17일 |
| 최초 릴리스 | 이 릴리스는 AWS Artifact을 도입했습니다. | 2016년 11월 30일 |

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