Add a permission의

AWS Artifact

AWS Artifact: Add a permission의

Table of Contents

AWS Artifact란 무엇인가요?

AWS Artifact 는 AWS 보안 및 규정 준수 문서의 온디맨드 다운로드를 제공합니다. 예를 들어,는 ISO(International Organization for Standardization) 표준 및 PCI(Payment Card Industry) 보안 표준 및 SOC(System and Organization Controls) 보고서 준수에 대한 보고서를 제공합니다. AWS Artifact 또한는 AWS 보안 제어의 구현 및 운영 효과를 검증하는 인증 기관의 인증 다운로드를 제공합니다.

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

또한 AWS Artifact 를 사용하여 조직의 여러 및에 AWS 대한 와의 계약 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 감사자 또는 규제 기관에 감사 아티팩트로 AWS Artifact 문서를 제출할 수 있습니다. 또한 이러한 감사 아티팩트를 지침으로 사용하여 자체 클라우드 아키텍처를 평가하고 회사 내부 제어의 효과를 평가할 수 있습니다. 감사 아티팩트에 대한 자세한 내용은 AWS Artifact FAQs.

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

가격 책정

AWS 는 AWS Artifact 문서와 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.

에 가입 AWS 계정

를 시작하려면이 AWS필요합니다 AWS 계정. 생성에 대한 자세한 AWS 계정내용은 AWS Account Management 참조 안내서의 시작하기 AWS 계정를 참조하세요.

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. 보고서를 다운로드하면 AWS Artifact보고서가 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 WorkDocs와 같은 안전한 공유 서비스를 이용하십시오. 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.

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

보고서 다운로드

1. https://console.aws.amazon.com/artifact/ AWS Artifact 콘솔을 엽니다.
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 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. (선택 사항) 이전 버전의 보고서를 다운로드하려면 보고서 제목을 선택하여 보고서의 세부 정보 페이지를 열 수 있습니다. 세부 정보 페이지에서 이전 버전 섹션을 찾고 원하는 버전 행에서 다운로드를 선택하여 보고서의 특정 버전을 다운로드합니다.
6. 보고서를 선택하고 보고서 다운로드를 선택합니다.
7. 다운로드하려는 특정 보고서에 대한 이용 약관(보고서 다운로드 조건 수락)을 수락하라는 메시지가 표시될 수 있습니다. 이용 약관을 자세히 읽는 것이 좋습니다. 읽기를 마치면 약관을 읽고 동의함을 선택한 다음 약관 수락 및 보고서 다운로드를 선택합니다.
8. 다운로드한 파일을 PDF 뷰어를 통해 엽니다. 동의 약관을 검토하고 아래로 스크롤하여 감사 보고서를 찾으십시오. 보고서에는 PDF 문서 내에 첨부 파일로 포함된 추가 정보가 있을 수 있으므로 PDF 파일 내의 첨부 파일에서 지원 문서를 확인해야 합니다. 첨부 파일을 보는 방법에 대한 지침은 섹션을 참조하세요PDF 문서의 첨부 파일 보기.

PDF 문서의 첨부 파일 보기

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

Adobe Acrobat Reader

https://get.adobe.com/reader/ Adobe 웹 사이트에서 최신 버전의 Adobe Acrobat Reader를 다운로드합니다.

Acrobat Reader에서 PDF 첨부 파일을 보는 방법에 대한 지침은 Adobe Support 웹 사이트의 PDFs의 링크 및 첨부 파일을 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 전환, 첨부 파일 표시를 선택합니다.

문서 보안 유지

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

지만, 사용자는 문서를 다운로드한 후 안전하게 보호할 책임이 AWS Artifact 있습니다.는 사용자가 문서를 다운로드하기 전에 이용 약관에 동의하도록 요구할 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 웹사이트에 올려서 이런 문서를 공유하면 안 됩니다. 문서를 다른 사람과 공유할 경우 Amazon WorkDocs 등과 같은 보안 문서 공유 서비스를 사용할 것을 적극 권장합니다. 이메일을 통해 문서를 보내거나 안전하지 않은 사이트에 업로드하지 마십시오.

문제 해결

문서를 다운로드할 수 없거나 오류 메시지가 표시되는 경우 AWS Artifact FAQ의 문제 해결을 참조하십시오.

에서 계약 관리 AWS Artifact

AWS Artifact 를 사용하여 AWS 계정 또는 조직의 계약을 검토하고 관리할 수 있습니다. 예를 들어 HIPAA(Health Insurance Portability and Accountability Act)의 적용을 받는 회사는 일반적으로 보호 대상 건강 정보(PHI)가 적절하게 보호되도록 AWS 하기 위해와 BAA(Business Associate Addendum) 계약을 체결해야 합니다. AWS Artifact 콘솔에서 이러한 계약을 검토하고 수락할 수 있으며, PHI를 합법적으로 처리할 수 AWS 계정 있는를 지정할 수 있습니다.

를 사용하는 경우 조직의 모든 사용자를 AWS대신하여 BAA와 같은 계약을 수락 AWS Organizations 할 수 AWS 계정 있습니다. 기존 및 이후의 모든 멤버 계정은 자동으로 계약을 적용받으며 합법적으로 PHI를 처리할 수 있습니다.

또한 AWS Artifact 를 사용하여 사용자 AWS 계정 또는 조직이 계약을 수락했는지 확인하고 수락된 계약의 조건을 검토하여 사용자의 의무를 이해할 수 있습니다. 계정 또는 조직이 더 이상 수락된 계약을 사용할 필요가 없는 경우를 사용하여 계약을 종료 AWS Artifact 할 수 있습니다. 계약을 종료했지만 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 및 페더레이션 사용자에게 필요한 권한이 있어야 합니다.

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

와 계약을 수락하려면 AWS

1. https://console.aws.amazon.com/artifact/ AWS Artifact 콘솔을 엽니다.
2. AWS Artifact 탐색 창에서 계약을 선택합니다.
3. 계정 계약 탭을 선택합니다.
4. https://console.aws.amazon.com/artifact/ AWS Artifact 콘솔을 엽니다.
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 다운로드를 위한 NDA 수락 대화 상자가 나타납니다.
8. 선택한 계약을 다운로드하려면 먼저 비밀 유지 계약(AWS Artifact NDA)의 AWS Artifact 약관에 동의해야 합니다.

   a. 보고서를 다운로드할 NDA 수락 대화 상자에서 AWS Artifact NDA를 검토합니다.

   b. (선택 사항) AWS Artifact NDA 사본을 인쇄하려면(또는 PDF로 저장하려면) NDA 인쇄를 선택합니다.

   c. NDA의 모든 조건을 읽었으며 이에 동의합니다를 선택합니다.

   d. AWS Artifact NDA를 수락하고 선택한 계약의 PDF를 다운로드하려면 NDA 수락 및 다운로드를 선택합니다.
9. PDF 뷰어에서 다운로드한 계약 PDF를 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 동의합니다를 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 종료할 수 있습니다. 그렇지 않으면 의 오프라인 계약 AWS Artifact 을 참조하십시오.

필수 권한

계약을 종료하려면 IAM 및 페더레이션 사용자에게 필요한 권한이 있어야 합니다.

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

와의 온라인 계약을 종료하려면 AWS

1. https://console.aws.amazon.com/artifact/ AWS Artifact 콘솔을 엽니다.
2. AWS Artifact 탐색 창에서 계약을 선택합니다.
3. 계정 계약 탭을 선택합니다.
4. 계약을 선택하고 계약 종료를 선택합니다.
5. 모든 확인란을 선택하여 계약 종료에 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 체결할 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. https://console.aws.amazon.com/artifact/ AWS Artifact 콘솔을 엽니다.
2. AWS Artifact 대시보드에서 계약을 선택합니다.
3. 조직 계약 탭을 선택합니다.
4. https://console.aws.amazon.com/artifact/ AWS Artifact 콘솔을 엽니다.
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 다운로드를 위한 NDA 수락 대화 상자가 나타납니다.
8. 선택한 계약을 다운로드하려면 먼저 비밀 유지 계약(AWS Artifact NDA)의 AWS Artifact 약관에 동의해야 합니다.

   a. 보고서를 다운로드할 NDA 수락 대화 상자에서 AWS Artifact NDA를 검토합니다.

   b. (선택 사항) AWS Artifact NDA 사본을 인쇄하려면(또는 PDF로 저장하려면) NDA 인쇄를 선택합니다.

   c. NDA의 모든 조건을 읽었으며 이에 동의합니다를 선택합니다.

   d. AWS Artifact NDA를 수락하고 선택한 계약의 PDF를 다운로드하려면 NDA 수락 및 다운로드를 선택합니다.
9. PDF 뷰어에서 다운로드한 계약 PDF를 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 동의합니다를 선택합니다.
    c. 계약 수락을 선택합니다.
12. 조직의 모든 기존 및 향후 계정에 대한 계약에 동의하려면 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 종료할 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 멤버 계정에 이를 전달해야 합니다. AWS Artifact 콘솔의 계약 페이지의 조직 계약에서 활성 조직 계약 목록을 볼 수 있습니다. https://console.aws.amazon.com/artifact/home?#!/agreements?tab=organizationAgreements

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

필수 권한

계약을 종료하려면 관리 계정 소유자에게 필요한 권한이 있어야 합니다.

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

AWS와의 온라인 조직 계약을 종료하려면

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

의 오프라인 계약 AWS Artifact

기존 오프라인 계약이 있는 경우 오프라인으로 수락한 계약이 AWS Artifact 표시됩니다. 예를 들면, 오프라인 비즈니스 관련자 부록(BAA)이 콘솔에 활성화 상태로 표시됩니다. 활성화 상태란 계약이 수락되었다는 의미입니다. 오프라인 계약을 종료하려면 계약에 포함된 종료 지침 및 설명을 확인하십시오.

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

에서 이메일 알림 구성 AWS Artifact

> **Note**
>
> 이 페이지의 내용은 commercial AWS Regions에만 적용되며 현재 에는 적용되지 않습니다 AWS GovCloud (US) Regions.

AWS Artifact 콘솔을 사용하여의 계약 및 보고서에 대한 업데이트에 대한 이메일 알림을 구성할 수 있습니다 AWS Artifact.는를 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 알림 수신자가 수신하는 알림을 지정하는 알림 설정에 대한 구성을 생성할 수 있습니다.

AWS Artifact 이메일 알림을 구성하려면 AWS Artifact 및에 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 알림 허브를 선택해야 합니다.

알림 허브를 선택하려면

1. AWS 사용자 알림 콘솔의 알림 허브 페이지를 엽니다.
2. AWS 사용자 알림 리소스를 저장할에서 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

> **Note**
>
> 이 페이지의 내용은 commercial AWS Regions에만 적용되며 현재 에는 적용되지 않습니다 AWS GovCloud (US) Regions.

사용자 알림 알림 허브를 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 및 모든(또는 일부) AWS Artifact 보고서에 대한 업데이트와 같이 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 보고서에서 AWS 보고서 업데이트를 선택한 상태로 유지합니다.
     a. 모든 보고서에 대한 알림을 받으려면 모든 보고서를 선택합니다.
     b. 특정 범주 및 시리즈의 보고서에 대해서만 알림을 받으려면 보고서 하위 집합을 선택합니다. 그런 다음 관심 있는 범주와 시리즈를 선택합니다.
   - 구성 이름에 구성의 이름을 입력합니다.
   - 이메일의 수신자에 AWS Artifact 알림 이메일을 수신할 이메일 주소 목록을 쉼표로 구분하여 입력합니다.
   - (선택 사항) 알림 구성에 태그를 추가하려면 태그를 확장하고 새 태그 추가를 선택한 다음 태그를 키-값 페어로 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 받습니다.

AWS Artifact 알림 설정에 대한 구성 편집

> **Note**
>
> 이 페이지의 내용은 commercial AWS Regions에만 적용되며 현재 에는 적용되지 않습니다 AWS GovCloud (US) Regions.

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. 편집할 구성을 선택합니다.
3. 편집을 선택합니다.
4. 구성 선택 및 필드를 편집합니다. 마쳤으면 변경 사항 저장을 선택합니다.

   새 이메일 주소를 알림 수신자로 추가한 경우는 해당 이메일 주소로 확인 이메일을 AWS 사용자 알림 보냅니다. 이메일 주소를 확인하려면 확인 이메일에서 수신자가 이메일 확인을 선택해야 합니다. 확인된 이메일 주소만 AWS Artifact 알림을 받습니다.

AWS Artifact 알림 설정에 대한 구성 삭제

> **Note**
>
> 이 페이지의 내용은 commercial AWS Regions에만 적용되며 현재 에는 적용되지 않습니다 AWS GovCloud (US) Regions.

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

구성 삭제

1. AWS Artifact 콘솔의 알림 설정 페이지를 엽니다.
2. 삭제할 구성을 선택합니다.
3. 삭제를 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 증명이며 리소스를 포함한 모든 AWS 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 사람과 공유하는 대신, 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 그 그룹에 IAM 사용자를 추가하면 여러 IAM 사용자에게 동일한 권한을 부여할 수 있습니다.

외부에서 사용자 자격 증명을 이미 관리하는 경우 IAM 사용자를 생성하는 대신 IAM 자격 증명 공급자를 사용할 AWS수 있습니다. 자세한 내용은 IAM 사용 설명서의 ID 공급자 및 페더레이션 섹션을 참조하세요.

내용

- 사용자에게에 대한 액세스 권한 부여 AWS Artifact
- 상용 AWS 리전 AWS Artifact 의에 대한 IAM 정책 예제
- AWS Artifact 의에 대한 IAM 정책 예제 AWS GovCloud (US) Regions
- 에 AWS 관리형 정책 사용 AWS Artifact
- 에 대한 서비스 연결 역할 사용 AWS Artifact
- AWS Artifact 보고서에 IAM 조건 키 사용

사용자에게에 대한 액세스 권한 부여 AWS Artifact

필요한 액세스 수준에 AWS Artifact 따라 사용자에게 권한을 부여하려면 다음 단계를 완료하세요.

작업

- 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 정책을 만들려면

다음 절차를 사용하여 IAM 사용자 및 그룹에 권한을 부여하는 데 사용할 수 있는 IAM 정책을 생성합니다.

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Policies를 선택합니다.
3. 정책 생성을 선택합니다.
4. JSON 탭을 선택합니다.
5. 정책 문서를 입력합니다. 정책을 직접 생성하거나 상용 AWS 리전 AWS Artifact 의에 대한 IAM 정책 예제의 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. 이 그룹에 언제든지 IAM 사용자를 추가할 수 있습니다.

IAM 그룹을 만들어 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 생성한 후 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.

상용 AWS 리전 AWS Artifact 의에 대한 IAM 정책 예제

IAM 사용자에게 권한을 부여하는 권한 정책을 생성합니다. 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.

이러한 정책은 commercial AWS Regions에 적용됩니다. 적용 가능한 정책은 AWS Artifact 의에 대한 IAM 정책 예제 AWS GovCloud (US) Regions를 AWS GovCloud (US) Regions참조하세요.

- 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

Example세분화된 권한을 통해 AWS 보고서를 관리하는 정책 예제

> **Tip**
>
> 정책을 직접 정의하는 대신 AWSArtifactReportsReadOnlyAccess 관리형 정책 사용을 고려하세요.

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

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

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

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Example타사 보고서를 관리하기 위한 정책 예시

> **Tip**
>
> 정책을 직접 정의하는 대신 AWSArtifactReportsReadOnlyAccess 관리형 정책 사용을 고려하세요.

타사 보고서는 IAM 리소스 `report`로 표시됩니다.

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:ListReports"
```

```
      ],
      "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 정책을 정의하는 대신 AWSArtifactAgreementsReadOnlyAccess 또는 AWSArtifactAgreementsFullAccess 관리형 정책을 사용하는 것을 고려해야 합니다.

Example계약 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/*"
    }
  ]
}
```

Example와 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:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
   },
   {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
      }
    }
 ]
}
```

Example관리 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:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
      }
    }
  ]
}
```

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

Example알림 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": [
        "*"
      ]
    }
  ]
}
```

AWS Artifact 의에 대한 IAM 정책 예제 AWS GovCloud (US) Regions

이러한 정책은 에만 적용됩니다 AWS GovCloud (US) Regions. commercial AWS Regions에 적용되는 정책은 상용 AWS 리전 AWS Artifact 의에 대한 IAM 정책 예제를 참조하세요.

IAM 사용자에게 권한을 부여하는 권한 정책을 생성합니다. 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.

- AWS 보고서를 관리하기 위한 정책 예제
- 계약 관리 정책 예시
- 와 통합할 정책 예제 AWS Organizations
- 관리 계정의 계약을 관리하기 위한 정책 예시
- 조직 계약을 관리하기 위한 정책 예시

Example보고서 관리 정책 예시

다음 정책은 모든 보고서를 다운로드할 수 있는 권한을 부여합니다.

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*"
    }
  ]
}
```

다음 정책은 SOC, PCI 및 ISO 보고서만 다운로드할 수 있는 권한을 부여합니다.

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

```
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Example계약 관리 정책 예시

다음 정책은 모든 계약을 다운로드할 수 있는 권한을 부여합니다. IAM 사용자는 이 권한이 있어야 계약을 수락할 수 있습니다.

```
{
  "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-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
```

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

Example와 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-us-gov: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:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EnableServiceTrustForArtifact",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "aws-artifact-account-sync.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Example관리 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-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
```

```
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
      }
    }
  ]
}
```

Example조직 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-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov: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"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

에 AWS 관리형 정책 사용 AWS Artifact

AWS 관리형 정책은에서 생성하고 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 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 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 줍니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용자 가이드의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSArtifactReportsReadOnlyAccess

`AWSArtifactReportsReadOnlyAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 보고서를 나열, 조회, 다운로드할 수 있는 ## ## 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

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

AWS 관리형 정책: AWSArtifactAgreementsReadOnlyAccess

`AWSArtifactAgreementsReadOnlyAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 AWS Artifact 서비스 계약을 나열하고 수락된 계약을 다운로드할 수 있는 ## ## 액세스 권한을 부여합니다. 여기에는 조직 세부 정보를 나열하고 설명할 수 있는 권한도 포함됩니다. 이 정책은 필요한 서비스 연결 역할이 존재하는지 확인하는 기능도 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 주체가 필요한 서비스 연결 역할이 존재하는지 확인할 수 있습니다.
- `organizations` - 보안 주체가 현재 조직을 설명하고 해당 조직에 대한 서비스 액세스를 나열할 수 있도록 허용합니다.

AWS 관리형 정책: AWSArtifactAgreementsFullAccess

`AWSArtifactAgreementsFullAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 AWS Artifact 계약을 나열, 다운로드, 수락 및 종료할 수 있는 ## 권한을 부여합니다. 또한 서비스에서 AWS 서비스 액세스를 나열 및 활성화 AWS Organizations 하고 조직 세부 정보를 설명할 수 있는 권한도 포함되어 있습니다. 또한이 정책은 필요한 서비스 연결 역할이 존재하는지 확인하는 기능을 제공하고 존재하지 않는 경우 생성합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `artifact` - 보안 주체가 계약을 나열, 다운로드, 수락 및 종료할 수 있도록 허용합니다 AWS Artifact.
- `iam` - 보안 주체가 필요한 서비스 연결 역할이 존재하는지 확인하고 존재하지 않는 경우 생성할 수 있습니다.
- `organizations` - 보안 주체가 현재 조직을 설명하고 해당 조직에 대한 서비스 액세스를 나열/활성화할 수 있도록 허용합니다.

AWS Artifact AWS 관리형 정책에 대한 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Artifact 이후부터의 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	설명	Date
AWSArtifactReports ReadOnlyAccess – 기존 정책에 대한 업데이트	AWS Artifact 는 보고서 버전을 나열할 수 있는 `artifact:ListReportVersions` 권한을 추가했습니다.	2025-12-15
AWS 계약 관리형 정책 업데이트	`organizations:EnableAWSServiceAccess` 권한 범위를 AWS Artifact의 서비스 보안 주체로 축소하도록 AWSArtifactAgreementsFullAccess 관리형 정책을 업데이트했습니다. 이는 관리형 정책의 기능에 영향을 주지 않습니다.	2025-10-16
AWS 보고서 관리형 정책 업데이트	AWSArtifactReports ReadOnlyAccess 관리형 정책을 업데이트하여 artifact:get 권한을 제거했습니다.	2025-03-21
AWS Agreements 관리형 정책 도입	AWSArtifactAgreementsReadOnlyAccess 및 AWSArtifactAgreementsFullAccess 관리형 정책을 도입했습니다.	2024-11-21
AWS Artifact 에서 변경 내용 추적 시작	AWS Artifact 는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했으며 AWSArtifactReportsReadOnlyAccess를 도입했습니다.	2023-12-15

에 대한 서비스 연결 역할 사용 AWS Artifact

AWS Artifact 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결된 고유한 유형의 IAM 역할입니다 AWS Artifact. 서비스 연결 역할은에서 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 않은 한 만 해당 역할을 수임 AWS Artifact 할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

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

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 AWS IAM으로 작업하는 서비스를 참조하고 서비스 연결 역할 열에서 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 AWSServiceRoleForArtifact라는 서비스 연결 역할을 사용합니다.는 AWS Artifact 를 통해 조직에 대한 정보를 수집할 수 있습니다 AWS Organizations.

AWSServiceRoleForArtifact 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `artifact.amazonaws.com`

AWSArtifactServiceRolePolicy라는 역할 권한 정책은가 `organizations` 리소스에서 다음 작업을 완료 AWS Artifact 하도록 허용합니다.

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

에 대한 서비스 연결 역할 생성 AWS Artifact

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. 조직 관리 계정의 조직 계약 탭으로 이동하여에서 시작하기 링크를 선택하면가 서비스 연결 역할을 AWS Management Console AWS Artifact 생성합니다.

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 선택하면가 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 연결 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 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**
>
> 리소스를 삭제하려고 할 때 AWS Artifact 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForArtifact에서 사용하는 AWS Artifact 리소스를 삭제하려면

1. AWS Artifact 콘솔에서 '조직 계약' 테이블 방문
2. 활성 조직 계약 종료

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForArtifact 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

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.

리전 이름	리전 자격 증명	에서 지원 AWS Artifact
미국 동부(버지니아 북부)	us-east-1	예
미국 동부(오하이오)	us-east-2	아니요
미국 서부(캘리포니아 북부)	us-west-1	아니요
미국 서부(오리건)	us-west-2	예
아프리카(케이프타운)	af-south-1	아니요
Asia Pacific (Hong Kong)	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

리전 이름	리전 자격 증명	에서 지원 AWS Artifact
중동(바레인)	me-south-1	아니요
중동(UAE)	me-central-1	아니요
남아메리카(상파울루)	sa-east-1	아니요
AWS GovCloud (US-East)	us-gov-east-1	아니요
AWS GovCloud(미국 서부)	us-gov-west-1	예

AWS Artifact 보고서에 IAM 조건 키 사용

IAM 조건 키를 사용하여 특정 보고서 범주 및 시리즈를 AWS Artifact기반으로 보고서에 대한 세분화된 액세스를 제공할 수 있습니다.

다음 예제 정책은 특정 보고서 범주와 시리즈를 기반으로 IAM 사용자에게 할당할 수 있는 권한을 보여 줍니다.

Example AWS 보고서 읽기 액세스를 관리하는 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 사용하면 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 사용하면 `Certifications and Attestations` 범주 및 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"
        }
      }
    }
  ]
}
```

를 사용하여 AWS Artifact API 호출 로깅 AWS CloudTrail

AWS Artifact 는 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다 AWS Artifact. CloudTrail은 AWS Artifact 에 대한 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Artifact 콘솔의 호출과 AWS Artifact API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 이벤트를 포함하여 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다 AWS Artifact. 추적을 구성하지 않은 경우에도 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 수행된 요청, 요청이 수행된 AWS Artifact IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 설명은 AWS CloudTrail 사용자 가이드를 참조하십시오.

AWS Artifact CloudTrail의 정보

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

에 대한 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 AWS Artifact생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 트레일을 생성하면 기본적으로 모든 AWS 리전에 트레일이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 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 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

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 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

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

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

AWS Artifact 로그 파일 항목 이해

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예에서는 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 표에는 AWS Artifact 사용 설명서의 AWS Artifact 릴리스 기록 및 관련 변경 사항이 나와 있습니다.

변경 사항	설명	날짜
ListReportVersions API에 대한 업데이트된 권한	예제 IAM 정책, 예제 GovCloud IAM 정책, AWSArtifactReportsReadOnlyAccess 관리형 정책, 새 ListReportVersions API를 수용하도록 보고서 버전 다운로드에 대한 `artifact:ListReportVersions` 권한 및 지원을 포함하도록 보고서 지침 다운로드를 업데이트했습니다. ListReportVersions	2025년 12월 15일
AWSArtifactAgreementsFullAccess 관리형 정책 업데이트	`organizations:EnableAWSServiceAccess` 권한 범위를 AWS Artifact의 서비스 보안 주체로 축소하도록 AWSArtifactReportsReadOnlyAccess 관리형 정책을 업데이트했습니다. 이는 관리형 정책의 기능에 영향을 주지 않습니다.	2025년 10월 16일
IAM 작업 사용 중단 알림 업데이트	AWS GovCloud (US) 파티션의 `artifact:DownloadAgreement` 및 `artifact:Get` 에 대한 IAM 작업 사용 중단 공지가 업데이트되었습니다.	2025년 7월 1일

AWS Artifact 의에 대한 세분화된 권한 AWS GovCloud (US) Regions	이제 AWS Artifact 기능이 모든 리전에 더 광범위하게 적용 가능하므로 제한 사항에 대한 참고 사항을 제거하면서 AWS GovCloud (US) Regions AWS Artifact 에서를 사용하기 위한 정책을 업데이트하고 확장했습니다.	2025년 3월 31일
AWSArtifactReportReadOnlyAccess 관리형 정책 업데이트	artifact:get 권한을 제거하도록 AWSArtifactReportsReadOnlyAccess 관리형 정책을 업데이트했습니다.	2025년 3월 21일
AWS Artifact 의에 대한 정책 예제 AWS GovCloud (US) Regions	AWS Artifact 에서 사용에 대한 예제 정책을 추가하고 AWS GovCloud (US) Regions AWS Artifact 에서 사용에 적용되지 않는 페이지를 기록했습니다 AWS GovCloud (US) Regions.	2024년 12월 6일
계약 실행, AWSArtifactAgreementsFullAccess 및 AWSArtifactAgreementsReadOnlyAccess 관리형 정책에 대한 세분화된 권한	AWS Artifact 계약 실행을 위한 세분화된 액세스를 활성화하고 AWSArtifactAgreementsFullAccess 및 AWSArtifactAgreementsReadOnlyAccess AWS 관리형 정책을 시작했습니다.	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 AWS Artifact API 참조, CloudTrail 로깅 설명서 및 자격 증명 및 액세스 관리 페이지를 관련 업데이트했습니다.	2023년 8월 1일
타사 보고서 - 일반적으로 사용 가능	API 참조 설명서 및 CloudTrail 로깅 설명서를 추가하고 타사 보고서를 정식으로 사용할 수 있도록 했습니다.	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 예제를 추가했습니다.	2022년 11월 30일
보안	혼동된 대리자 방지를 위해 자격 증명 및 액세스 관리 페이지에 섹션을 추가했습니다.	2021년 12월 20일
Reports	비밀 유지 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
AWS GovCloud (US) 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.