사용자 가이드

AWS Artifact

AWS Artifact: 사용자 가이드

Table of Contents

AWS Artifact란 무엇인가요?

AWS Artifact은(는) AWS ISO 인증, PCI (지불 카드 산업) 보고서, SOC(Service Organization Controls) 보고서와 같은 AWS 보안 및 규정 준수 문서를 온디맨드로 다운로드할 수 있습니다. 이러한 보안 및 규정 준수 문서(감사 아티팩트)를 감사 기관이나 규제 기관에 제출하여 귀사에서 사용하는 AWS 인프라와 서비스에 대한 보안 및 규정 준수를 입증할 수 있습니다. 이러한 문서는 또한 자체 클라우드 아키텍처를 조사하고 회사의 내부 관리가 효율적인지 평가하는 데 지침으로 사용할 수도 있습니다.

또한 AWS Artifact에서는 AWS Marketplace에서 제품을 판매하는 독립 소프트웨어 개발 판매 회사(ISV)의 ISO 인증 및 SOC(Service Organization Controls) 보고서와 같은 보안 및 규정 준수 문서를 온디맨드로 다운로드할 수 있습니다. 자세한 내용은 AWS Marketplace공급업체 통찰력을 참조하십시오.

회사의 보안과 규정 준수를 입증하는 문서를 작성하거나 갖추는 것은 AWS 고객의 책임입니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

또한 AWS Artifact을(를) 사용하여 비즈니스 관련자 부록(BAA)과 같은 AWS 계약의 상태를 검토, 수락 및 추적할 수 있습니다. 미국 건강 보험 양도 및 책임에 관한 법(HIPAA)의 적용을 받는 기업에서는 일반적으로 보호 대상 건강 정보(PHI)를 적절히 보호하기 위해 BAA가 필요합니다. AWS Artifact로 AWS와의 계약을 수락하고 제한된 정보를 합법적으로 처리할 수 있는 AWS 계정을 지정할 수 있습니다. 여러 계정을 대신하여 계약을 수락할 수 있습니다. 여러 계정에 대한 계약을 수락하려면 AWS Organizations으로 조직을 생성하십시오.

자세한 내용은 AWS Artifact 섹션을 참조하세요.

요금

AWS은(는) AWS Artifact 문서와 계약서를 무료로 제공합니다.

다음으로 시작하기 AWS Artifact

AWS Artifact 다음과 같은 중앙 리소스를 제공합니다. AWS 보안 및 규정 준수 보고서. 아티팩트는 다음에서 사용할 수 있습니다. AWS Artifact 서비스 조직 제어 (SOC) 보고서, 결제 카드 업계 (PCI) 보고서, 구현 및 운영 효율성을 검증하는 인증 기관의 인증이 포함됩니다. AWS 보안 통제. 또한, AWS Artifact 제품을 판매하는 독립 소프트웨어 공급업체 () 의 ISO 인증 및 서비스 조직 제어 (SOC) 보고서와 같은 보안 및 규정 준수 문서에 대한 온디맨드 액세스를 제공합니다. ISVs AWS Marketplace. 자세한 내용은 을 참조하십시오. AWS Marketplace 공급업체 인사이트.

AWS Artifact 비즈니스 제휴 부록 () BAA 과 같은 법적 계약을 수락하고 관리할 수 있습니다. 사용하는 경우 AWS Organizations조직 내 모든 계정을 대신하여 계약을 수락할 수 있습니다. 수락하면 기존 및 이후의 모든 멤버 계정에 자동으로 계약이 적용됩니다.

Tasks

- 1단계: 가입 AWS
- 2단계: 보고서 다운로드
- 3단계: 계약 관리
- 4단계: 알림 관리

1단계: 가입 AWS

가지고 있지 않은 경우 AWS 계정다음 단계를 완료하여 새로 만드세요.

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/등록 열기.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   가입할 때 AWS 계정, 그리고 AWS 계정 루트 사용자생성됩니다. 루트 사용자는 모두에 액세스할 수 있습니다. AWS 서비스 및 계정 내 리소스 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

2단계: 보고서 다운로드

Adobe Acrobat Reader를 사용하여 보고서를 다운로드할 수 있습니다. 다른 PDF 리더는 지원되지 않습니다. 자세한 내용은 보고서 다운로드 단원을 참조하십시오.

보고서 다운로드

1. 여십시오. AWS Artifact 에서 콘솔을 https://console.aws.amazon.com/artifact/실행하세요.
2. 에서 AWS Artifact 홈페이지에서 보고서 보기를 선택합니다.
3. 보고서 페이지에서 다음을 사용하십시오. AWS 보고서 탭을 사용하여 액세스할 수 있습니다. AWS 보고서 (예: SOC 1/2/3PCI, C5 등) 를 선택하고 타사 보고서 탭으로 이동하여 해당 제품을 판매하는 독립 소프트웨어 공급업체 (ISVs) 의 보고서에 액세스할 수 있습니다. AWS Marketplace.
4. (선택 사항) 보고서를 찾으려면 검색 필드에 키워드를 입력합니다. 보고서 제목, 범주, 시리즈, 설명 등 개별 열을 기반으로 보고서에 대한 대상 검색을 수행할 수 있습니다. 예를 들어 클라우드 컴퓨팅 규정 준수 제어 카탈로그 (C5) 보고서를 찾아야 하는 경우 “포함” 연산자와 “C5"라는 용어를 사용하여 “제목” 열을 검색할 수 있습니다.
5. 보고서를 선택하고 보고서 다운로드를 선택합니다.
6. (선택 사항) 타사 보고서 탭에서 보고서 제목을 클릭하여 보고서의 세부 정보 페이지에 액세스하여 ISV 보고서에 대해 자세히 알아볼 수 있습니다.
7. 다운로드 중인 특정 보고서에 적용되는 이용 약관에 동의를 요청하는 메시지가 표시될 수 있습니다. 주의해서 면밀히 읽으십시오. 작성을 마치면 약관을 읽었으며 이에 동의합니다를 선택한 다음 약관 동의 및 보고서 다운로드를 선택합니다.
8. 다운로드한 파일을 PDF 뷰어를 통해 엽니다. 동의 약관을 검토하고 아래로 스크롤하여 감사 보고서를 찾으십시오. 보고서에는 PDF 문서에 첨부 파일로 포함된 추가 정보가 있을 수 있으므로 지원 문서를 위해 PDF 파일 내에 첨부 파일이 있는지 확인하십시오. 첨부 파일을 보는 방법에 대한 지침은 여기에서 확인하십시오.

타사 보고서는 다음과 같은 경우에만 액세스할 수 있습니다. AWS 에 가입한 고객 AWS Marketplace 공급업체 인사이트. 자세한 내용은 섹션을 참조하십시오.AWS Marketplace 공급업체 인사이트.

3단계: 계약 관리

계약을 체결하기 전에 다음 약관을 다운로드하여 동의해야 합니다. AWS Artifact 비밀 유지 계약 (NDA). 각 계약은 기밀이며 회사 외부의 다른 사람과 공유할 수 없습니다.

와의 계약을 수락하려면 AWS

1. 여십시오. AWS Artifact 에서 콘솔을 https://console.aws.amazon.com/artifact/실행하세요.
2. 에서 AWS Artifact 탐색 창에서 계약을 선택합니다.
3. 계정에 대한 계약을 관리하려면 계정 계약을 선택하고, 조직을 대신하여 계약을 관리하려면 조직 계약을 선택하십시오.
4. 계약 섹션을 확장합니다.
5. 다운로드 및 검토를 선택합니다.
6. 이용 약관를 읽어보십시오. 작업이 완료되면 수락 및 다운로드를 선택합니다.
7. 계약을 검토한 다음 동의함을 나타내는 확인란을 선택합니다.
8. 동의를 선택하여 계약을 수락합니다.

자세한 내용은 계약 관리 단원을 참조하십시오.

4단계: 알림 관리

새 보고서 및 계약의 가용성 또는 기존 보고서 및 계약의 업데이트에 대한 알림을 구독할 수 있습니다. AWSArtifact는 AWS 사용자 알림 서비스를 사용하여 알림을 보냅니다. 알림은 알림 구성 설정 중에 사용자가 제공하는 이메일 주소로 전송됩니다.

구성 생성

1. AWS사용자 알림 서비스에서 알림 허브 페이지를 엽니다.
2. AWS사용자 알림 리소스를 저장할 지역을 선택합니다. 기본적으로 사용자 알림 데이터는 미국 동부(버지니아 북부)에 저장되며 선택한 다른 리전에 복제됩니다. 자세한 내용은 알림 허브 설명서를 참조하십시오.
3. 구성 만들기를 클릭합니다.
4. 계약 알림을 받으려면 계약 업데이트 확인란을 클릭하십시오. AWS
5. 보고서에 대한 알림을 받으려면 보고서 업데이트 확인란을 클릭합니다. AWS 특정 범주 및 시리즈의 보고서에 대한 알림만 받으려면 보고서 하위 집합 확인란을 클릭하고 관심 있는 범주 및 시리즈의 확인란을 클릭하십시오.
6. 구성 이름을 입력합니다.
7. 알림을 보내야 하는 이메일 목록을 쉼표로 구분하여 입력합니다.

8. (선택 사항) 알림 구성에 태그를 할당하려면 태그 섹션을 확장하여 키-값 쌍을 입력합니다. 참고: 태그는 AWS 리소스에 할당할 수 있는 레이블이며 각 태그는 키와 사용자가 정의할 수 있는 선택적 값으로 구성됩니다. 태그는 리소스 관리, 검색 및 필터링에 도움이 됩니다.
9. 제출을 클릭합니다.
10. 제공된 이메일 주소로 확인 이메일이 전송되며, 이메일 수신자는 전송된 확인 이메일에 있는 이메일 확인 링크를 클릭해야 합니다. 단, 확인된 이메일 주소만 알림을 받기 시작한다는 점에 유의하세요.

자세한 내용은 알림 관리 단원을 참조하십시오.

에서 보고서 다운로드 AWS Artifact

AWS Artifact 콘솔에서 보고서를 다운로드할 수 있습니다. 에서 AWS Artifact보고서를 다운로드하면 보고서가 자동으로 생성되며 모든 보고서에는 고유한 워터마크가 있습니다. 따라서 신뢰할 수 있는 사람과만 보고서를 공유해야 합니다. 보고서를 이메일에 첨부하여 보내거나 온라인으로 공유하지 마십시오. 보고서를 공유하려면 Amazon과 같은 안전한 공유 서비스를 사용하십시오 WorkDocs. 일부 보고서를 다운로드하려면 먼저 이용 약관에 동의해야 합니다.

내용

보고서 다운로드

보고서를 다운로드하려면 필요한 권한이 있어야 합니다. 자세한 내용은 AWS Artifact의 ID 및 액세스 관리 단원을 참조하십시오.

AWS Artifact가입하면 일부 보고서를 다운로드할 수 있는 권한이 계정에 자동으로 부여됩니다. 액세스에 AWS Artifact문제가 있는 경우 AWS Artifact 서비스 인증 참조 페이지의 지침을 따르세요.

보고서 다운로드

1. 에서 AWS Artifact 콘솔을 https://console.aws.amazon.com/artifact/여십시오.
2. AWS Artifact 홈페이지에서 보고서 보기를 선택합니다.
3. 보고서 페이지에서 보고서 탭을 사용하여 AWS AWS 보고서 (예: SOC 1/2/3PCI, C5 등) 에 액세스하고 타사 보고서 탭으로 이동하여 제품을 판매하는 독립 소프트웨어 공급업체 (ISVs) 의 보고서에 액세스할 수 있습니다. AWS Marketplace
4. (선택 사항) 보고서를 찾으려면 검색 필드에 키워드를 입력합니다. 보고서 제목, 범주, 시리즈, 설명 등 개별 열을 기반으로 보고서에 대한 대상 검색을 수행할 수 있습니다. 예를 들어 클라우드 컴퓨팅 규정 준수 제어 카탈로그 (C5) 보고서를 찾아야 하는 경우 “포함” 연산자와 “C5"라는 용어를 사용하여 “제목” 열을 검색할 수 있습니다.
5. 보고서를 선택하고 보고서 다운로드를 선택합니다.

6. (선택 사항) 타사 보고서 탭에서 보고서 제목을 클릭하여 보고서의 세부 정보 페이지에 액세스하여 ISV 보고서에 대해 자세히 알아볼 수 있습니다.
7. 다운로드 중인 특정 보고서에 적용되는 이용 약관에 동의를 요청하는 메시지가 표시될 수 있습니다. 주의해서 면밀히 읽으십시오. 작성을 마치면 약관을 읽었으며 이에 동의합니다를 선택한 다음 약관 동의 및 보고서 다운로드를 선택합니다.
8. 다운로드한 파일을 PDF 뷰어를 통해 엽니다. 동의 약관을 검토하고 아래로 스크롤하여 감사 보고서를 찾으십시오. 보고서에는 PDF 문서에 첨부 파일로 포함된 추가 정보가 있을 수 있으므로 지원 문서를 위해 PDF 파일 내에 첨부 파일이 있는지 확인하십시오. 첨부 파일을 보는 방법에 대한 지침은 여기에서 확인하십시오.

PDF문서 내 첨부 파일 보기

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

Adobe Acrobat 뷰어

1. 여기에서 최신 버전의 Adobe Acrobat을 다운로드하십시오.
2. Adobe Acrobat 뷰어에서 파일을 엽니다.
3. [첨부 파일] 패널을 열려면 PDF 문서 왼쪽의 종이클립 아이콘을 클릭하거나 [보기] > [표시/숨기기] > [탐색 창] > [첨부 파일] 을 선택합니다.
4. 첨부 파일 패널에서 첨부 파일을 두 번 클릭하여 문서를 확인합니다.

Firefox 브라우저

1. 여기에서 Firefox 브라우저를 다운로드하십시오.
2. [PDF파일] 메뉴의 [파일 열기] 옵션을 사용하여 Firefox 브라우저에서 파일을 엽니다.
3. 첨부 파일을 열려면 화면 왼쪽 상단의 토글 사이드바 아이콘을 클릭합니다.

문서 보안 유지

AWS Artifact 문서는 기밀이므로 항상 안전하게 보관해야 합니다. AWS Artifact 문서에 AWS 공동 책임 모델을 사용합니다. AWS 즉, AWS 클라우드에 있는 동안에는 문서를 안전하게 보관할 책임이 있지만 다운로드한 후에는 문서를 안전하게 유지할 책임이 있습니다. AWS Artifact 문서를 다운로드하려면 먼저 이용 약관에 동의해야 할 수도 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. WorkDocsAmazon과 같은 안전한 문서 공유 서비스를 사용하여 다른 사람과 문서를 공유하는 것이 좋습니다. 이메일을 통해 문서를 보내거나 안전하지 않은 사이트에 업로드하지 마십시오.

문제 해결

문서를 다운로드할 수 없거나 오류 메시지를 받는 경우 의 문제 해결을 참조하십시오 AWS Artifact FAQ.

AWS Artifact에서의 계약 관리

AWS Artifact 계약을 통해 AWS Management Console을(를) 사용해 계정 또는 조직에 관한 계약을 검토하고 수락하며 관리할 수 있습니다. 예를 들어, 미국 건강 보험 양도 및 책임에 관한 법(HIPAA)의 적용을 받는 기업에서는 일반적으로 보호 대상 건강 정보(PHI)를 적절히 보호하기 위해 비즈니스 관련자 부록(BAA) 계약이 필요합니다. AWS Artifact을(를) 사용하면 AWS을(를) 통해 BAA와 같은 계약을 수락하고, PHI를 합법적으로 처리할 수 있는 AWS 계정을 지정할 수 있습니다. AWS Organizations을(를) 사용할 경우 조직 내 모든 계정을 대신하여 AWS BAA 같은 계약을 수락할 수 있습니다. 기존 및 이후의 모든 멤버 계정은 자동으로 계약을 적용받으며 합법적으로 PHI를 처리할 수 있습니다.

또한 AWS Artifact을(를) 사용하여 AWS 계정 또는 조직이 계약을 수락했는지 확인하고, 의무 사항을 이해하기 위해 수락한 계약 조건을 검토할 수 있습니다. 수락한 계약을 더 이상 계정 또는 조직에서 사용할 필요가 없게 되면 AWS Artifact을(를) 통해 계약을 종료할 수 있습니다. 계약을 해지했지만 나중에 계약이 필요하다고 판단되면 다시 활성화할 수 있습니다.

목차

AWS Artifact에서의 단일 계정의 계약 관리

AWS Organizations에서 조직 내 멤버 계정이라 하더라도 본인 계정의 계약은 수락할 수 있습니다. AWS Organizations에 대한 자세한 내용은 AWS Organizations사용 설명서를 참조하세요.

AWS와(과)의 계약 수락

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

필요한 권한

한 계정의 관리자인 경우 IAM 사용자 및 역할이 있는 페더레이션 사용자에게 계약 한 개 또는 여러 개를 액세스하고 관리할 수 있는 권한을 부여할 수 있습니다. 기본적으로 관리자 권한이 있는 사용자만 계약을 수락할 수 있습니다. 계약을 수락하려면 IAM 및 페더레이션 사용자에게 반드시 다음 권한이 있어야 합니다.

```
artifact:DownloadAgreement
```

```
artifact:AcceptAgreement
```

자세한 내용은 자격 증명 및 액세스 관리 섹션을 참조하세요.

AWS와(과)의 계약을 수락하려면

1. https://console.aws.amazon.com/artifact/에서 AWS Artifact 콘솔을 엽니다.
2. AWS Artifact 탐색 창에서 계약을 선택합니다.
3. 계정 계약 탭을 선택합니다.
4. 계약 섹션을 확장합니다.
5. 다운로드 및 검토를 선택합니다.
6. 이용 약관를 읽어보십시오. 작업이 완료되면 수락 및 다운로드를 선택합니다.
7. 계약을 검토한 다음 동의함을 나타내는 확인란을 선택합니다.
8. 본인 계정에 해당하는 계약을 수락하려면 적용을 선택합니다.

AWS와(과)의 계약 종료

계약을 수락하는 데 AWS Artifact 콘솔을 사용한 경우에는 콘솔을 사용하여 해당 계약을 종료할 수 있습니다. 그렇지 않으면 오프라인 계약 을 참조하십시오.

필요한 권한

계약을 종료하려면 IAM 및 페더레이션 사용자에게 반드시 다음 권한이 있어야 합니다.

```
artifact:TerminateAgreement
```

자세한 내용은 자격 증명 및 액세스 관리 섹션을 참조하세요.

AWS와(과)의 온라인 계약을 종료하려면

1. https://console.aws.amazon.com/artifact/에서 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.

AWS Artifact에서의 다중 계정의 계약 관리

AWS Organizations 조직의 관리 계정 소유자인 경우 조직 내 모든 계정을 대신해서 계약을 수락할 수 있습니다. 조직 계약을 수락하거나 종료할 수 있는 올바른 AWS Artifact 권한이 있는 관리 계정으로 로그인해야 합니다. `organizations:DescribeOrganization` 권한이 있는 멤버 계정의 사용자는 자신을 대신해서 누군가 수락한 조직 계약을 볼 수 있습니다.

조직에 속하지 않은 계정의 경우 AWS Organizations사용 설명서의 조직 생성 및 관리에서 설명하는 대로 조직을 생성하거나 조직에 가입할 수 있습니다.

AWS Organizations은(는) 통합 결제 기능과 모든 기능이라는 두 가지 기능 모음을 제공합니다. 조직에 AWS Artifact을(를) 사용하려면 소속 조직에 대해 모든 기능이 활성화되어 있어야 합니다. 조직에 통합 결제만 구성된 경우 AWS Organizations사용 설명서의 조직 내 모든 기능 활성화를 참조하십시오.

조직에서 삭제된 멤버 계정에는 해당 조직 계약이 더 이상 적용되지 않습니다. 필요한 경우 멤버 계정이 새 계약을 체결할 수 있도록 관리 계정 관리자는 조직에서 멤버 계정을 삭제하기 전에 이 사실을 해당 멤버 계정에게 알려줘야 합니다. 유효한 조직 계약의 목록은 AWS Artifact조직 계약에서 볼 수 있습니다.

자세한 내용은 AWS Organizations사용 설명서의 조직 내 AWS 계정 관리를 참조하십시오.

조직에 대한 계약 수락

AWS Organizations에서는 조직 내 모든 멤버 계정을 대신하여 계약을 수락할 수 있습니다. 계약을 수락하기 전에 귀사의 법무, 개인정보 보호, 규정 준수 팀과 협의할 것을 권장합니다.

필요한 권한

계약을 수락하려면 관리 계정의 소유자에게 다음과 같은 권한이 있어야 합니다.

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

자세한 내용은 자격 증명 및 액세스 관리 섹션을 참조하세요.

조직에 대한 계약을 수락하려면

1. https://console.aws.amazon.com/artifact/에서 AWS Artifact 콘솔을 엽니다.
2. AWS Artifact 대시보드에서 계약을 선택합니다.
3. 조직 계약 탭을 선택합니다.
4. 계약 섹션을 확장합니다.
5. 다운로드 및 검토를 선택합니다.
6. 이용 약관를 읽어보십시오. 작업이 완료되면 수락 및 다운로드를 선택합니다.
7. 계약을 검토한 다음 동의함을 나타내는 확인란을 선택합니다.
8. 기존 및 미래 모든 조직 내 계정에 대하여 계약을 수락하려면 적용을 선택합니다.

조직 계약 종료

AWS Artifact 콘솔로 조직 내 모든 멤버 계정을 대신하여 계약을 수락한 경우 그 콘솔을 사용하여 해당 계약을 종료할 수 있습니다. 그렇지 않으면 오프라인 계약 을 참조하십시오.

필요한 권한

계약을 종료하려면 관리 계정의 소유자에게 다음과 같은 권한이 있어야 합니다.

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

자세한 내용은 자격 증명 및 액세스 관리 섹션을 참조하십시오.

AWS와의 온라인 조직 계약을 종료하려면

1. https://console.aws.amazon.com/artifact/에서 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.

AWS Artifact에서의 기존 오프라인 계약 관리

기존 오프라인 계약이 있는 경우 오프라인으로 수락한 계약이 AWS Artifact에 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.

AWS Organizations 조직에서 관리 계정 소유자인 경우, AWS Artifact을(를) 사용하여 조직 내 모든 계정에 오프라인 계약 조건을 적용할 수 있습니다. 오프라인에서 수락한 계약을 조직과 조직 내 모든 계정에 적용하려면 다음 권한이 있어야 합니다.

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

조직 내 멤버 계정 소유자인 경우 다음 권한이 있어야 오프라인 조직 계약을 볼 수 있습니다.

```
organizations:DescribeOrganization
```

자세한 내용은 자격 증명 및 액세스 관리 섹션을 참조하세요.

AWS Artifact에서의 알림 관리

AWS Artifact 알림을 사용하면 이메일 알림을 설정할 수 있습니다. 알림 설정 페이지에서 아래에 설명된 대로 알림을 구독하고 기타 알림 설정을 관리할 수 있습니다. AWS Artifact는 AWS 사용자 알림 서비스를 사용하여 알림을 전송합니다. AWS Artifact 알림을 사용하려면 AWS Artifact 및 AWS 사용자 알림 서비스에 필요한 권한을 갖고 있어야 합니다. 자세한 내용은 자격 증명 및 액세스 관리 섹션을 참조하세요.

목차

알림 설정

알림 수신을 시작하려면 먼저 사용자 알림 데이터를 저장할 리전을 지정해야 합니다. 알림 허브를 설정하려면 아래 단계를 따르십시오.

알림 허브를 설정하려면

1. AWS 사용자 알림 서비스에서 알림 허브 페이지를 엽니다.
2. AWS 사용자 알림 리소스를 저장할 리전을 선택합니다. 기본적으로 사용자 알림 데이터는 미국 동부(버지니아 북부) 에 저장되며 선택한 다른 리전에 복제됩니다. 자세한 내용은 알림 허브 설명서를 참조하십시오.
3. 제출을 클릭합니다.

알림을 구독하려면

1. AWS Artifact 알림 설정 페이지를 엽니다.
2. AWS Artifact의 알림을 구독하려면 아티팩트 알림 구독 토글을 클릭하십시오.

알림 구독을 취소하려면

1. AWS Artifact 알림 설정 페이지를 엽니다.
2. AWS Artifact에서 알림 구독을 취소하려면 Artifact 알림 구독 토글을 클릭하십시오.

구성 생성

1. AWS Artifact 알림 설정 페이지를 엽니다.
2. 구성 생성을 클릭합니다.
3. 계약 알림을 받으려면 AWS 계약 업데이트 옆의 확인란을 선택한 상태로 유지하십시오.
4. 보고서 알림을 받으려면 AWS 보고서 업데이트 옆의 확인란을 선택한 상태로 유지하십시오.
5. 모든 보고서에 대한 알림을 받으려면 모든 보고서 옆의 확인란을 선택한 상태로 유지하십시오.
6. 특정 카테고리 및 시리즈의 보고서에 대해서만 알림을 받으려면 보고서 하위 집합 확인란을 클릭하십시오. 그런 다음 관심 있는 카테고리와 시리즈의 확인란을 클릭합니다.
7. 구성 이름을 입력합니다.
8. 알림을 보내야 하는 이메일 목록을 쉼표로 구분하여 입력합니다.
9. (선택 사항) 알림 구성에 태그를 할당하려면 태그 섹션을 확장하여 키-값 쌍을 입력합니다. 참고: 태그는 AWS 리소스에 할당할 수 있는 레이블이며, 각 태그는 사용자가 정의할 수 있는 키 및 선택적 값으로 구성됩니다. 태그는 리소스 관리, 검색 및 필터링에 도움이 됩니다.
10. 구성 생성을 클릭합니다.
11. 제공된 이메일 주소로 확인 이메일이 전송되며, 이메일 수신자는 전송된 확인 이메일에 있는 이메일 확인 링크를 클릭해야 합니다. 단, 확인된 이메일 주소만 알림을 받기 시작한다는 점에 유의하세요.

구성을 편집하려면

1. AWS Artifact 알림 설정 페이지를 엽니다.
2. 편집하려는 구성 행을 클릭합니다.
3. 페이지 오른쪽 위에서 편집 버튼을 클릭합니다.
4. 모든 필드를 편집할 수 있습니다. 변경 사항이 만족스러우면 변경사항 저장을 선택하십시오.
5. 새 이메일 주소를 추가한 경우 각 이메일 주소로 확인 이메일이 발송됩니다. 확인 이메일에 있는 이메일 확인 링크를 클릭합니다.

구성을 삭제하려면

1. AWS Artifact 알림 설정 페이지를 엽니다.
2. 삭제하려는 구성 행을 클릭합니다.
3. 삭제를 클릭합니다.

4. 경고 메시지를 읽은 후 삭제를 클릭합니다.

태그를 구성에 할당하기

태그란 AWS 리소스에 할당되는 레이블을 말합니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다. 태그는 리소스 관리, 검색 및 필터링에 도움이 됩니다. 구성을 만들거나 편집할 때 선택적으로 태그를 설정할 수 있습니다. 자세한 내용은 리소스 태깅을 참조하십시오.

문제 해결

AWS Artifact 알림을 사용하는 동안 오류 메시지를 수신하는 경우 AWS Artifact FAQ의 문제 해결을 참조하십시오.

AWS Artifact의 ID 및 액세스 관리

AWS에 가입할 때 AWS 계정과 연결된 이메일 주소 및 암호를 입력합니다. 이 두 가지가 루트 자격 증명이며 AWS Artifact에 대한 리소스를 포함하여 모든 AWS 리소스에 대한 전체 액세스 권한을 제공합니다. 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 다른 사람과 자격 증명을 공유하는 대신, AWS Artifact의 문서 또는 계약서에 액세스해야 하는 사람들과 나 자신에 대해 IAM 사용자라는 특별한 사용자 자격 증명을 생성하도록 합니다. 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.

AWS 외부에서 사용자 자격 증명을 이미 관리하고 있다면, IAM 사용자를 생성하는 대신 IAM 자격 증명 공급자를 사용할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 ID 공급자 및 페더레이션 섹션을 참조하세요.

내용

AWS Artifact에 대한 사용자 액세스 설정

다음 단계를 완료하여 필요한 액세스 수준에 따라 사용자에게 AWS Artifact에 대한 권한을 부여하십시오.

Tasks

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 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. JSON 탭을 선택합니다.
5. 정책 문서를 입력합니다. 정책을 직접 생성하거나 예제 IAM 정책의 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 Console액세스 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.

세분화된 권한으로 마이그레이션

AWS이제 Artifact를 통해 고객은 세분화된 권한을 사용할 수 있습니다. 고객은 이러한 세분화된 권한을 통해 약관 동의 및 보고서 다운로드와 같은 기능에 대한 액세스 권한을 세밀하게 제어할 수 있습니다.

세분화된 권한을 통해 보고서에 액세스하려면 AWSArtifactReportsReadOnlyAccess관리형 정책을 활용하거나 아래 권장 사항에 따라 권한을 업데이트할 수 있습니다. 이전에 세분화된 권한 사용을 옵트아웃한 경우 보고서 콘솔에서 제공되는 “Artifact AWS 보고서에 대한 세분화된 권한 선택” 링크를 사용하여 옵트인해야 합니다.

새 권한으로 업데이트하는 데 문제가 있는 경우 콘솔에서 제공되는 “AWSArtifact 보고서에 대한 세분화된 권한 거부” 링크를 통해 이전 권한으로 보고서에 액세스할 수 있습니다.

새 권한으로 마이그레이션

리소스 비특정 권한 마이그레이션

사용자는 기존 권한이 포함된 기존 정책을 세분화된 권한이 포함된 정책으로 교체해야 합니다.

기존 정책:

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

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

세분화된 권한이 포함된 새 정책:

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

특정 리소스 권한 마이그레이션

사용자는 기존 권한이 포함된 기존 정책을 세분화된 권한이 포함된 정책으로 교체해야 합니다. 보고서 리소스 와일드카드 권한이 조건 키로 대체되었습니다.

기존 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 권한과 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"
          ]
        }
      }
```

```
    }
  ]
}
```

예제 IAM 정책

IAM 사용자에게 권한을 부여하는 권한 정책을 생성합니다. 사용자에게 AWS Artifact 보고서에 대한 액세스 권한을 부여하고 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 예시
- 타사 보고서를 관리하기 위한 정책 예시
- 계약 관리 정책 예시
- 통합할 정책 예시 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 예제 정책

> **Tip**
>
> 정책을 직접 정의하는 대신 AWSArtifactReportsReadOnlyAccess 관리형 정책을 사용하는 것을 고려해야 합니다.

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, PCI 및 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**
>
> 정책을 직접 정의하는 대신 AWSArtifactReportsReadOnlyAccess 관리형 정책을 사용하는 것을 고려해야 합니다.

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: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"
      ]
    }
  ]
}
```

Example 계약 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:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

다음 정책은 계약을 수락할 수 있는 권한을 부여합니다.

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

```
      ]
    }
  ]
}
```

다음 정책은 계약을 종료할 수 있는 권한을 부여합니다.

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

다음 정책은 단일 계정 계약을 관리할 권한을 부여합니다.

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

Example 통합할 정책 예시 AWS Organizations

다음 정책은 통합에 AWS Artifact 사용되는 IAM 역할을 생성할 권한을 부여합니다. AWS Organizations조직의 관리 계정은 이들 권한이 있어야 조직 계약을 시작할 수 있습니다.

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

다음 정책은 사용 권한을 AWS Artifact 부여할 권한을 부여합니다. AWS Organizations조직의 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": [
    {
      "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": "*"
    }
  ]
}
```

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

다음 정책은 조직 계약을 볼 수 있는 권한을 부여합니다.

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

AWS Artifact에 대한 AWS 관리형 정책

AWS 관리형 정책은 AWS에서 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

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

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

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` - AWS Artifact에서 보고서를 나열, 조회, 다운로드할 수 있는 보안 주체를 허용합니다.

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

AWS 관리형 정책에 대한 Artifact 업데이트

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

변경 사항	설명	날짜
Artifact, 변경 사항 추적 시작	Artifact가 AWS 관리형 정책에 대한 변경 내용 추적을 시작했고 AWSArtifactReports	2023-12-15

변경 사항	설명	날짜
	ReadOnlyAccess가 도입되었습니다.	

AWS Artifact에 서비스 연결 역할 사용

AWS Artifact는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 AWS Artifact에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS Artifact에서 사전 정의하며, 서비스에서 사용자를 대신하여 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 AWS Artifact를 더 쉽게 설정할 수 있습니다. AWS Artifact는 서비스 연결 역할의 권한을 정의하며, 별도로 정의하지 않는 한 AWS Artifact만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 AWS Artifact 리소스를 보호합니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS Artifact에 대한 서비스 연결 역할 권한

AWS Artifact는 AWSServiceRoleForArtifact라는 서비스 연결 역할을 사용합니다. 즉, AWS Artifact가 AWS Organizations 서비스를 통해 조직에 대한 정보를 수집할 수 있도록 합니다.

AWSServiceRoleForArtifact 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `artifact.amazonaws.com`

AWSArtifactServiceRolePolicy라는 역할 권한 정책을 사용하면 AWS Artifact가 `organizations` 리소스에 대해 다음 작업을 완료할 수 있습니다.

- `DescribeOrganization`
- `DescribeAccount`

- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

AWS Artifact에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. 조직 관리 계정의 조직 계약 탭으로 이동하여 AWS Management Console에서 "시작하기" 링크를 선택하면 AWS Artifact가 서비스 연결 역할을 생성합니다.

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

AWS Artifact에 대한 서비스 연결 역할 편집

AWS Artifact에서는 AWSServiceRoleForArtifact 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 객체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AWS Artifact에 대한 서비스 연결 역할 삭제

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 삭제하려 할 때 AWS Artifact 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하십시오.

AWSServiceRoleForArtifact에서 사용하는 AWS Artifact 리소스 삭제

1. AWS Artifact 콘솔의 "조직 계약" 표를 참조하십시오.
2. 활성 조직 계약 종료

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

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

AWS Artifact 서비스 연결 역할이 지원되는 리전

AWS Artifact는 서비스가 제공되는 모든 리전에서 서비스 연결 역할을 사용하도록 지원하지 않습니다. 다음 리전에서 AWSServiceRoleForArtifact 역할을 사용할 수 있습니다.

지역명	리전 자격 증명	AWS Artifact에서의 지원
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(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

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

IAM 조건 키 사용

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

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

Example AWS 보고서 읽기 액세스 관리 정책 예시

AWS Artifact 보고서는 IAM 리소스 `report`로 표시됩니다.

다음 정책은 `Certifications and Attestations` 범주에 속하는 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 정책은 SOC 시리즈에 속하는 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 정책은 `Certifications and Attestations` 범주를 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"
        }
      }
    }
  ]
}
```

AWS CloudTrail을 사용하여 AWS Artifact API 호출 로깅

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

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 AWS Artifact 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. AWS Artifact에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AWS Artifact에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 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 Artifact는 CloudTrail 로그 파일에 다음 작업을 이벤트로 로깅합니다.

- ListReports
- GetAccountSettings

- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings

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

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

AWS Artifact 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 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"
    }
  ]
}
```

AWS Artifact에 대한 문서 기록

다음 표에서는 AWS Artifact의 릴리스를 설명합니다.

변경 사항	설명	날짜
세분화된 보고서 액세스 및 AWSArtifactReportReadOnlyAccess 관리형 정책	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 설명서가 추가되고 AWS Artifact 및 AWS Organizations 통합에 대한 정책 예시가 업데이트되었습니다.	2023년 9월 26일
알림	알림 관리에 대한 설명서를 게시하고 API 참조 가이드, CloudTrail 로깅 설명서, AWS Artifact ID 및 액세스 관리 페이지를 적절히 업데이트했습니다.	2023년 8월 1일
타사 보고서 - 일반적으로 사용 가능	API 참조 설명서, CloudTrail 로깅 설명서를 추가하고 타사 보고서를 일반적으로 사용할 수 있도록 했습니다.	2023년 1월 27일
타사 보고서(미리 보기)	AWS Marketplace에서 제품을 판매하는 독립 소프트웨어 개발 판매 회사(ISV)에 대한 규정 준수 보고서를 출시했습니다. 또한 타사 보고서에 대한 ID 및	2022년 11월 30일

	액세스 관리 페이지에 정책 예시를 추가했습니다.	
보안	ID 및 액세스 관리 페이지에 혼란스러운 부정 행위 방지를 위한 섹션을 추가했습니다.	2021년 12월 20일
보고서	비밀 유지 계약을 제거하고 보고서 다운로드에 대한 약관을 도입했습니다.	2020년 12월 17일
홈페이지 및 검색	보고서 및 계약 페이지에 서비스 홈 페이지 및 검색 표시줄을 추가했습니다.	2020년 5월 15일
GovCloud 출시	GovCloud 리전에서 AWS Artifact을(를) 출시했습니다.	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.