AWS Artifact

사용 설명서

AWS Artifact: 사용 설명서

Table of Contents

AWS Artifact란 무엇입니까?

AWS Artifact는 온디맨드 다운로드AWSAWS ISO 인증, PCI (결제 카드 산업), SOC (서비스 조직 제어) 보고서와 같은 보안 및 규정 준수 문서 이러한 보안 및 규정 준수 문서(감사 자료)를 감사 기관이나 규제 기관에 제출하여 귀사에서 사용하는 AWS 인프라와 서비스에 대한 보안 및 규정 준수를 입증할 수 있습니다. 또한 이러한 문서를 자체 클라우드 아키텍처를 평가하고 자사의 내부 통제의 효과성을 평가하기 위한 지침으로 사용할 수 있습니다. AWS Artifact은(는) AWS에 관한 문서만을 제공합니다. AWS 고객은 자사의 보안 및 규정 준수 상태를 입증할 수 있는 문서를 개발하거나 확보할 책임이 있습니다. 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 정보는 AWS Artifact을 참조하십시오.

요금

AWS에서 제공합니다AWS Artifact문서와 계약서를 무료로 제공합니다.

AWS Artifact 시작하기

AWS Artifact에서는 AWS 보안 및 규정 준수 보고서를 위한 중앙 리소스를 제공합니다. 에서 사용할 수 있는 아티팩트AWS Artifact서비스 조직 제어 (SOC) 보고서, PCI (결제 카드 산업) 보고서, AWS 보안 제어의 구현 및 운영 효율성을 검증하는 인증 기관의 인증이 포함됩니다.AWS Artifact을 (를) 사용하여 비즈니스 관련자 부록 (BAA) 과 같은 법적 계약을 수락하고 관리할 수 있습니다. AWS Organizations을 사용할 경우 조직 내 모든 계정을 대신하여 계약을 수락할 수 있습니다. 수락하면 기존 및 이후의 모든 멤버 계정에 자동으로 계약이 적용됩니다.

작업

1단계: AWS에 가입

AWS 계정이 없는 경우 다음 절차에 따라 계정을 생성합니다.

AWS 계정에 가입하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

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

2단계: 보고서 다운로드

Adobe Acrobat Reader를 사용하여 보고서를 다운로드할 수 있습니다. 다른 PDF 리더는 지원하지 않습니다. 자세한 정보는 보고서 다운로드 (p. 4)을 참조하십시오.

보고서 다운로드

1. 열기AWS Artifact콘솔https://console.aws.amazon.com/artifact/.
2. 온AWS Artifact홈 페이지, 선택보고서 보기.
3. (선택 사항) 검색 필드에 키워드를 입력하여 보고서를 찾습니다.
4. 보고서를 선택한 다음보고서 다운로드.
5. 수락하라는 메시지가 표시될 수 있습니다.이용 약관다운로드 중인 특정 보고서에 적용됩니다. 단원을 면밀히 읽어보는 것이 좋습니다. 작업을 마쳤으면 [] 를 선택합니다.모든 약관을 읽었으며 이에 동의합니다.다음 를 선택합니다.약관 수락 및 다운로드.
6. 다운로드한 파일을 Adobe Acrobat Reader를 사용하여 엽니다. 읽기이용 약관섹션 작업을 마쳤으면 지침에 따라 다운로드한 보고서를 확인합니다.

3단계: 계약 관리

계약 체결하기 전에 계약 조건을 다운로드하여 동의해야 합니다.AWS Artifact비공개 계약 (NDA). 각 계약은 기밀로 유지되며 회사 외부의 다른 사용자와 공유할 수 없습니다.

AWS와(과)의 계약을 수락하려면

1. 열기AWS Artifact콘솔https://console.aws.amazon.com/artifact/.
2. AWS Artifact 탐색 창에서 Agreements(계약)을 선택합니다.
3. 선택계정 계약계정에 대한 계약 관리조직 계약조직을 대신하여 계약을 관리합니다.
4. 계약 부분을 확장합니다.
5. Download and review(다운로드 및 검토)를 선택합니다.
6. 읽기이용 약관. 작업을 마쳤으면 [] 를 선택합니다.수락 및 다운로드.
7. 계약 검토한 다음 동의함을 나타내는 확인란을 선택합니다.
8. 선택Accept계약을 수락합니다.

자세한 내용은 계약 관리 (p. 6) 단원을 참조하세요.

에서 보고서 다운로드AWS Artifact

AWS Artifact 콘솔에서 보고서를 다운로드할 수 있습니다. AWS Artifact에서 보고서를 다운로드하면 전용 보고서가 생성되며 모든 보고서에는 고유한 워터마크가 찍힙니다. 따라서 신뢰할 수 있는 사람과만 보고서를 공유해야 합니다. 보고서를 이메일에 첨부하여 보내거나 온라인으로 공유하지 마십시오. 보고서를 공유하려면 Amazon WorkDocs와 같은 보안 공유 서비스를 이용하십시오. 일부 보고서에서는 다음을 수락해야 합니다.이용 약관다운로드하기 전에

목차

보고서 다운로드

보고서를 다운로드하려면 필수 권한이 있어야 합니다. 자세한 정보는 AWS Artifact의 자격 증명 및 액세스 관리 (p. 10)을 참조하십시오.

AWS Artifact에 가입하면 일부 보고서에 대한 다운로드 권한이 귀하의 계정에 자동으로 부여됩니다. 목록의 다른 보고서에 액세스하도록 요청하려면 제공된 양식을 사용하여 AWS에서 액세스를 요청하십시오.

보고서 다운로드

1. 열기AWS Artifact에서 콘솔https://console.aws.amazon.com/artifact/.
2. 온AWS Artifact홈 페이지, 선택보고서 보기.
3. (선택 사항) 검색 필드에 키워드를 입력하여 보고서를 찾습니다.
4. 보고서를 선택한 다음보고서 다운로드.
5. 수락하라는 메시지가 표시될 수 있습니다.이용 약관다운로드 중인 특정 보고서에 적용됩니다. 주의해서 면밀히 읽으십시오. 작업을 마쳤으면 [] 를 선택합니다.모든 약관을 읽었으며 이에 동의합니다.를 선택한 다음약관 수락 및 다운로드.
6. Adobe Acrobat Reader를 사용하여 다운로드한 파일을 엽니다. 읽기이용 약관섹션 작업을 마쳤으면 지침에 따라 다운로드한 보고서를 확인합니다.

문서 보안

AWS Artifact문서는 기밀이므로 항상 보안을 유지해야 합니다.AWS Artifact는 이러한 문서에 대해 AWS 공동 책임 모델을 사용합니다. 이는 다음을 의미합니다.AWS문서에 있는 동안 문서를 안전하게 유지할 책임이 있습니다.AWS클라우드를 다운로드한 후에 보안을 유지할 책임은 고객에게 있습니다.AWS Artifact수락해야 할 수도 있습니다.이용 약관문서를 다운로드하기 전에 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 WorkDocs와 같은 보안 문서 공유 서비스를 사용할 것을 적극 권장합니다. 문서를 이메일로 보내거나 보안이 유지되지 않는 사이트에 업로드하지 마십시오.

문제 해결

문서를 다운로드할 수 없거나 오류 메시지가 표시되면 [] 를 참조하십시오.문제 해결의AWS ArtifactFAQ.

계약 관리AWS Artifact

AWS Artifact 계약을 통해 AWS Management Console을 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 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 Artifact를 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 되면AWS Artifact계약을 종료하려면 계약을 종료했지만 나중에 필요하다는 사실을 알게 되면 계약을 다시 활성화할 수 있습니다.

목차

에서 단일 계정에 대한 계약 관리AWS Artifact

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

와의 계약 수락AWS

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

필수 권한

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

```
artifact:DownloadAgreement
artifact:AcceptAgreement
```

자세한 정보는 Identity and Access Management (p. 10)을 참조하십시오.

AWS와(과)의 계약을 수락하려면

1. 열기AWS Artifact콘솔https://console.aws.amazon.com/artifact/.
2. AWS Artifact 탐색 창에서 Agreements(계약)을 선택합니다.
3. Account agreements(계정 계약) 탭을 선택합니다.
4. 계약 부분을 확장합니다.
5. Download and review(다운로드 및 검토)를 선택합니다.
6. 읽기이용 약관. 마쳤으면 를 선택합니다.수락 및 다운로드.
7. 계약을 검토한 다음 동의함을 나타내는 확인란을 선택합니다.
8. 선택Accept를 사용하여 계정에 대한 계약을 수락합니다.

와의 계약 종료AWS

계약을 수락하는 데 AWS Artifact 콘솔을 사용한 경우에는 콘솔을 사용하여 해당 계약을 종료할 수 있습니다. 그렇지 않으면 오프라인 계약 (p. 8) 단원을 참조하십시오.

필수 권한

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

```
artifact:TerminateAgreement
```

자세한 정보는 Identity and Access Management (p. 10)을 참조하십시오.

AWS와(과)의 온라인 계약을 종료하려면

1. 열기AWS Artifact콘솔https://console.aws.amazon.com/artifact/.
2. AWS Artifact 탐색 창에서 Agreements(계약)을 선택합니다.
3. Account agreements(계정 계약) 탭을 선택합니다.
4. 계약을 선택하고계약 종료.
5. 모든 확인란을 선택하여 계약 종료에 동의함을 나타냅니다.
6. [Terminate]를 선택합니다. 확인 메시지가 나타나면 종료(Terminate)를 선택합니다.

에서 여러 계정에 대한 계약 관리AWS Artifact

관리 계정의 소유자인 경우AWS Organizations조직 내 모든 계정을 대신하여 계약을 수락할 수 있습니다. 올바른 계정을 사용하여 관리 계정에 로그인해야 합니다.AWS Artifact조직 계약을 수락하거나 종료할 수 있는 권한입니다. `describeOrganizations` 권한이 있는 멤버 계정의 사용자는 자신을 대신해서 누군가 수락한 조직 계약을 볼 수 있습니다.

조직에 속하지 않은 계정의 경우, 지침에 따라 조직을 생성하거나 조직에 가입할 수 있습니다.조직 생성 및 관리의AWS Organizations사용 설명서.

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. 조직에서 통합 결제에 대해서만 구성된 경우조직 내 모든 기능 활성화의AWS Organizations사용 설명서.

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. 활성 조직 계약 목록은 에서 볼 수 있습니다.AWS Artifact조직 계약.

자세한 내용은 단원을 참조하십시오.조직의 AWS 계정 관리의AWS Organizations사용 설명서.

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.

필수 권한

계약을 수락하려면 관리 계정의 소유자에게 다음과 같은 권한이 있어야 합니다.

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
```

```
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateRole
iam:AttachRolePolicy
```

자세한 정보는 Identity and Access Management (p. 10)을 참조하십시오.

조직에 대한 계약을 수락하려면

1. 열기AWS Artifact콘솔https://console.aws.amazon.com/artifact/.
2. AWS Artifact 대시보드에서 Agreements(계약)을 선택합니다.
3. Organization agreements(조직 계약) 탭을 선택합니다.
4. 계약 부분을 확장합니다.
5. Download and review(다운로드 및 검토)를 선택합니다.
6. 읽기이용 약관. 마쳤으면 를 선택합니다.수락 및 다운로드.
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 (p. 8) 단원을 참조하십시오.

필수 권한

계약을 종료하려면 관리 계정의 소유자에게 다음과 같은 권한이 있어야 합니다.

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateRole
iam:AttachRolePolicy
```

자세한 정보는 Identity and Access Management (p. 10)을 참조하십시오.

AWS와의 온라인 조직 계약을 종료하려면

1. 열기AWS Artifact콘솔https://console.aws.amazon.com/artifact/.
2. AWS Artifact 대시보드에서 Agreements(계약)을 선택합니다.
3. Organization agreements(조직 계약) 탭을 선택합니다.
4. 계약을 선택하고계약 종료.
5. 모든 확인란을 선택하여 계약 종료에 동의함을 나타냅니다.
6. [Terminate]를 선택합니다. 확인 메시지가 나타나면 종료(Terminate)를 선택합니다.

에서 기존 오프라인 계약 관리AWS Artifact

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. 오프라인오프라인 계약을 종료하려면 계약에 포함된 종료 지침 및 설명을 확인하십시오.

계정이 관리 계정인 경우AWS Organizations조직, 사용할 수 있습니다AWS Artifact를 사용하여 조직 내 모든 계정에 오프라인 계약 조건을 적용합니다. 오프라인에서 수락한 계약을 조직과 조직 내 모든 계정에 적용하려면 다음 권한이 있어야 합니다.

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateRole
iam:AttachRolePolicy
```

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

```
organizations:DescribeOrganization
```

자세한 내용은 Identity and Access Management (p. 10) 단원을 참조하세요.

AWS Artifact의 자격 증명 및 액세스 관리

AWS에 가입할 때 AWS 계정과 연결된 이메일 주소 및 암호를 입력합니다. 이것들은 당신입니다루트 자격 증명을 사용하면 모든 사용자에 대한 전체 액세스를 제공합니다.AWS리소스 (리소스 포함)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.

에 로그인하는 대신AWS루트 자격 증명이 있는 계정 또는 다른 사람과 자격 증명을 공유하는 경우IAM 사용자본인 및 문서 또는 계약서에 액세스해야 할 수 있는 모든 사용자를 위해AWS 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 ID를 이미 관리하는 경우AWS, IAM을 사용할 수 있습니다자격 증명 공급자IAM 사용자를 생성하는 대신 자세한 내용은 단원을 참조하십시오.자격 증명 공급자 및 페더레이션의IAM 사용 설명서.

IAM 사용자를 생성하고 액세스 권한을 부여합니다.AWS Artifact

사용자에게 에 대한 권한을 부여하려면 다음 단계를 완료하십시오AWS Artifact필요한 액세스 수준을 기반으로 합니다.

작업

- 1단계: IAM 정책을 생성합니다. (p. 10)
- 2단계: IAM 그룹을 만들어 정책을 연결하려면 (p. 11)
- 3단계: IAM 사용자를 생성하여 그룹에 추가합니다. (p. 11)

1단계: IAM 정책을 생성합니다.

IAM 관리자는 권한을 부여하는 정책을 생성할 수 있습니다.AWS Artifact작업 및 리소스.

IAM 정책을 만들려면

다음 절차에 따라 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. [Create policy]를 선택합니다.
4. JSON 탭을 선택합니다.
5. 정책 문서를 입력합니다. 본인의 정책을 생성하거나 의 정책 중 하나를 사용할 수 있습니다.예제 IAM 정책 (p. 11).
6. 정책 검토를 선택합니다. 정책 검사기가 모든 구문 오류를 보고합니다.
7. 온정책 검토페이지에서 정책의 목적을 기억하는 데 도움이 되는 고유한 이름을 입력합니다. 설명을 입력할 수도 있습니다.
8. 정책 생성(Create policy)을 선택합니다.

2단계: IAM 그룹을 만들어 정책을 연결하려면

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

IAM 그룹을 생성하여 정책을 연결하려면

1. 탐색 창에서 그룹을 선택한 다음, 새 그룹 생성을 선택합니다.
2. 용그룹 이름를 선택하고 그룹 이름을 입력한 다음다음 단계.
3. [검색] 필드에 생성한 정책의 이름을 입력합니다. 정책의 확인란을 선택하고다음 단계.
4. 그룹 이름 및 정책을 검토합니다. 준비가 되면 를 선택합니다.그룹 생성.

3단계: IAM 사용자를 생성하여 그룹에 추가합니다.

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

IAM 사용자를 생성하여 그룹에 추가하려면

1. 탐색 창에서 사용자(Users)와 사용자 추가(Add user)를 차례로 선택합니다.
2. 용사용자 이름를 선택하면 하나 이상의 사용자에 대한 이름을 입력합니다.
3. AWS Management Console 액세스(console access) 옆의 확인란을 선택합니다. 자동 생성 또는 사용자 지정 암호를 구성합니다. 선택적으로 선택할 수 있습니다.사용자는 다음 로그인 시 새 암호를 생성해야 함사용자가 처음 로그인할 때 암호 재설정을 요구합니다.
4. [다음: 권한(Next: Permissions)]을 선택합니다.
5. 선택그룹에 사용자 추가를 선택하고 만든 그룹을 선택합니다.
6. [다음: 권한(Next: Tags)]를 선택합니다. 선택적으로 사용자에게 태그를 추가할 수 있습니다.
7. [다음: 권한(Next: Review)]를 선택합니다. 준비가 되면 를 선택합니다.사용자 생성.

예제 IAM 정책

IAM 사용자에게 권한을 부여하는 권한 정책을 생성할 수 있습니다. 사용자에게 액세스 권한을 부여할 수 있습니다.AWS Artifact보고서와 단일 계정 또는 조직을 대신하여 계약을 수락하고 다운로드하는 기능

다음 정책은 필요한 액세스 수준에 따라 IAM 사용자에게 할당할 수 있는 권한을 보여 줍니다.

Example 보고서 관리를 위한 정책의 예

다음 정책은 모든 보고서를 다운로드할 수 있는 권한을 부여합니다.

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

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

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

```
{
    "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/*"
            ]
        }
    ]
}
```

Example 계약 관리를 위한 정책의 예

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 계약서에 동의할 수 있는 권한을 부여합니다.

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

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

다음 정책은 계약을 해지할 수 있는 권한을 부여합니다.

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

다음 정책은 단일 계정 계약을 관리할 수 있는 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 예제AWS Organizations

다음 정책은 다음과 같은 IAM 역할을 생성할 수 있는 권한을 부여합니다AWS Artifact통합하는 데 사용합니다.AWS Organizations. 조직 계약을 시작하려면 조직의 관리 계정에 이러한 권한이 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "arn:aws:iam::*:role/*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateRole",
```

```
            "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync"
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync",
            "Condition": {
                "ArnEquals": {
                    "iam:PolicyARN": "arn:aws:iam::aws:policy/service-role/
AWSArtifactAccountSync"
                }
            }
        }
    ]
}
```

다음 정책은 부여에 대한 권한을 부여합니다AWS Artifact를 사용할 권한AWS Organizations. 조직 계약을 시작하려면 조직의 관리 계정에 이러한 권한이 있어야 합니다.

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

Example 관리 계정에 대한 계약을 관리하는 정책의 예

다음 정책은 관리 계정에 대한 계약을 관리할 수 있는 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:CreateRole",
            "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync",
            "Condition": {
                "ArnEquals": {
                    "iam:PolicyARN": "arn:aws:iam::aws:policy/service-role/
AWSArtifactAccountSync"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization"

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

Example 조직 계약을 관리할 정책의 예

다음 정책은 조직 계약을 관리할 수 있는 권한을 부여합니다. 필요한 권한이 있는 다른 사용자는 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": "*"
        }
    ]
}
```

교차 서비스 혼동된 대리자 예방

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. InAWS교차 서비스 가장으로 인해 혼동된 대리자 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 호출할 때 발생할 수 있습니다. 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

사이에 신뢰할 수 있는 액세스를 활성화하는 경우AWS Artifact과AWS Organizations사용자 계정에 해당 역할을 수임할 수 있는 사용자를 제한하는 정책을 사용하여 자동으로 역할을 생성합니다.

우리는 를 사용합니다.`aws:SourceArn`과`aws:SourceAccount`트러스트 정책의 전역 조건 컨텍스트 키를 사용하여 계정에서 만든 서비스 역할을 맡을 수 있는 엔터티를 제한합니다. 전역 조건 컨텍스트 키를 사용하면`aws:SourceAccount`가치와 계정`aws:SourceArn`동일한 정책 문에서 사용되는 경우 value는 동일한 계정 ID를 사용해야 합니다.

다음은 신뢰할 수 있는 액세스를 활성화할 때 역할로 만든 정책의 예입니다.AWS Artifact과AWS Organizations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "aws-artifact-account-sync.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnEquals": {
                  "aws:SourceArn": "arn:aws:artifact:us-west-2:00117294401"
                },
                "StringEquals": {
                  "aws:SourceAccount": "00117294401"
                }
            }
        }
    ]
}
```

AWS Artifact에 대한 문서 기록

다음 표에서는 AWS Artifact의 릴리스를 설명합니다.

update-history-change	update-history-description	update-history-date
[Security (p. 17)]	혼동 대리인 방지를 위해 ID 및 액세스 관리 페이지에 섹션을 추가했습니다.	2021년 12월 20일
보고서 (p. 17)	기밀 유지 계약이 제거되고 보고서 다운로드에 대한 약관이 도입되었습니다.	2020년 12월 17일
홈 페이지 및 검색 (p. 17)	보고서 및 계약 페이지에 서비스 홈 페이지와 검색 창을 추가했습니다.	2020년 5월 15일
GovCloud 출시 (p. 17)	출시AWS ArtifactGovCloud 지역에서 사용할 수 있습니다.	2019년 11월 7일
AWS Organizations계약 (p. 17)	조직에 대한 계약 관리를 위한 지원이 추가되었습니다.	2018년 20월 6일
계약 (p. 17)	관리 지원 추가AWS Artifact계약.	2017년 6월 17일
최초 릴리스 (p. 17)	이 릴리스는 AWS Artifact을 도입했습니다.	2016년 11월 30일

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