AWS Artifact

Panduan Pengguna

AWS Artifact: Panduan Pengguna

Table of Contents

Apa itu AWS Artifact?

AWS Artifact menyediakan unduhan sesuai permintaan untuk dokumen keamanan dan kepatuhan AWS, seperti sertifikasi ISO AWS, Industri Kartu Pembayaran (PCI), dan laporan Kontrol Organisasi Layanan (SOC). Anda dapat mengirimkan dokumen keamanan dan kepatuhan (juga dikenal sebagai Artefak audit) kepada auditor atau regulator Anda untuk menunjukkan keamanan dan kepatuhan infrastruktur dan layanan AWS yang Anda gunakan. Anda juga dapat menggunakan dokumen-dokumen ini sebagai pedoman untuk mengevaluasi arsitektur cloud Anda sendiri dan menilai keefektifan kontrol internal perusahaan Anda. AWS Artifact hanya menyediakan dokumen tentang AWS. Pelanggan AWS bertanggung jawab untuk menyusun atau memperoleh dokumen yang menunjukkan keamanan dan kepatuhan perusahaan mereka. Untuk informasi selengkapnya, lihat Model Tanggung Jawab Bersama.

Anda juga dapat menggunakan AWS Artifact untuk meninjau, menerima, dan melacak status perjanjian AWS seperti Perjanjian Rekanan Bisnis (BAA). BAA biasanya diperlukan untuk perusahaan yang tunduk pada Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) untuk memastikan bahwa informasi kesehatan yang dilindungi (PHI) dijaga dengan benar. Dengan AWS Artifact, Anda dapat menerima perjanjian dengan AWS dan menetapkan akun AWS yang secara legal dapat memproses informasi yang dibatasi. Anda dapat menerima perjanjian atas nama beberapa akun. Untuk menerima perjanjian untuk beberapa akun, gunakan AWS Organizations untuk membuat sebuah organisasi.

Untuk informasi selengkapnya, lihat AWS Artifact.

Harga

AWS menyediakan dokumen dan perjanjian AWS Artifact untuk Anda secara gratis.

Memulai dengan AWS Artifact

AWS Artifact menyediakan sumber daya pusat untuk laporan keamanan dan kepatuhan AWS. Artefak yang tersedia di AWS Artifact mencakup laporan Kontrol Organisasi Layanan (SOC), laporan Industri Kartu Pembayaran (PCI), dan sertifikasi dari badan akreditasi yang memvalidasi pelaksanaan dan efektivitas operasi kontrol keamanan AWS. AWS Artifact memungkinkan Anda untuk menerima dan mengelola perjanjian legal seperti Perjanjian Rekanan Bisnis (BAA). Jika Anda menggunakan AWS Organizations, Anda dapat menerima perjanjian atas nama semua akun dalam organisasi Anda. Ketika diterima, semua akun anggota yang ada dan yang akan datang secara otomatis tercakup dalam perjanjian.

Tugas

Langkah 1: Daftar AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah berikut untuk membuatnya.

Untuk mendaftar ke Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Langkah 2: Mengunduh laporan

Anda dapat mengunduh laporan menggunakan Adobe Acrobat Reader. Pembaca PDF lainnya tidak didukung. Untuk informasi lebih lanjut, lihat Mengunduh laporan (p. 4).

Untuk mengunduh laporan

1. Buka konsol AWS Artifact pada https://console.aws.amazon.com/artifact/.
2. Pada halaman beranda AWS Artifact, pilih Lihat laporan.
3. (Opsional) Masukkan kata kunci di kolom pencarian untuk menemukan laporan.
4. Pilih laporan, lalu pilih Unduh laporan.
5. Anda mungkin diminta untuk menyetujui Syarat dan Ketentuan yang berlaku untuk laporan tertentu yang Anda unduh. Kami sarankan Anda membacanya dengan saksama. Setelah selesai, pilih Saya telah membaca dan menyetujui semua syarat lalu pilih Terima syarat dan unduh.
6. Buka file yang diunduh menggunakan Adobe Acrobat Reader. Baca bagian Syarat dan Ketentuan. Setelah selesai, ikuti petunjuk untuk melihat laporan unduhan.

Langkah 3: Mengelola perjanjian

Sebelum Anda terikat dalam perjanjian, Anda harus mengunduh dan menyetujui persyaratan perjanjian kerahasiaan (NDA) AWS Artifact. Setiap perjanjian bersifat rahasia dan tidak boleh dibagikan dengan orang lain di luar perusahaan Anda.

Untuk menerima perjanjian dengan AWS

1. Buka konsol AWS Artifact pada https://console.aws.amazon.com/artifact/.
2. Pada panel navigasi AWS Artifact, pilih Perjanjian.
3. Pilih Perjanjian akun untuk mengelola perjanjian untuk akun Anda atau Perjanjian organisasi untuk mengelola perjanjian atas nama organisasi Anda.
4. Perluas bagian perjanjian.
5. Pilih Unduh dan tinjau.
6. Baca Syarat dan Ketentuan. Setelah selesai, pilih Terima dan unduh.
7. Tinjau perjanjian, kemudian pilih kotak centang untuk menunjukkan bahwa Anda setuju.
8. Pilih Terima untuk menerima perjanjian.

Untuk informasi lebih lanjut, lihat Mengelola perjanjian (p. 6).

Mengunduh laporan di AWS Artifact

Anda dapat mengunduh laporan dari konsol AWS Artifact. Saat mengunduh laporan dari AWS Artifact, laporan dihasilkan khusus untuk Anda, dan setiap laporan memiliki watermark yang unik. Maka dari itu, Anda hanya boleh berbagi laporan ini dengan orang-orang yang Anda percaya. Jangan lampirkan laporan dalam email dan jangan bagikan secara online. Untuk berbagi laporan, gunakan layanan berbagi yang aman seperti Amazon WorkDocs. Beberapa laporan mengharuskan Anda untuk menyetujui Syarat dan Ketentuan sebelum Anda dapat mengunduhnya.

Daftar Isi

Mengunduh laporan

Untuk mengunduh laporan, Anda harus memiliki izin yang diperlukan. Untuk informasi lebih lanjut, lihat Identity and access management di AWS Artifact (p. 10).

Saat Anda mendaftar ke AWS Artifact, akun Anda secara otomatis diberikan izin untuk mengunduh beberapa laporan. Jika Anda perlu meminta akses ke laporan lain yang ada di daftar, gunakan formulir yang disediakan untuk meminta akses dari AWS.

Untuk mengunduh laporan

1. Buka konsol AWS Artifact pada https://console.aws.amazon.com/artifact/.
2. Pada halaman beranda AWS Artifact, pilih Lihat laporan.
3. (Opsional) Masukkan kata kunci di kolom pencarian untuk menemukan laporan.
4. Pilih laporan, lalu pilih Unduh laporan.
5. Anda mungkin diminta untuk menyetujui Syarat dan Ketentuan yang berlaku untuk laporan tertentu yang Anda unduh. Kami sarankan Anda membacanya dengan saksama. Setelah selesai, pilih Saya telah membaca dan menyetujui semua syarat lalu pilih Terima syarat dan unduh.
6. Buka file yang diunduh menggunakan Adobe Acrobat Reader. Baca bagian Syarat dan Ketentuan. Setelah selesai, ikuti petunjuk untuk melihat laporan yang diunduh.

Mengamankan dokumen Anda

Dokumen AWS Artifact bersifat rahasia dan harus tetap aman setiap saat. AWS Artifact menggunakan model tanggung jawab bersama AWS untuk dokumennya. Ini berarti bahwa AWS bertanggung jawab untuk menjaga dokumen tetap aman saat berada di AWS Cloud, tetapi Anda bertanggung jawab untuk menjaga keamanannya setelah Anda mengunduhnya. AWS Artifact mungkin mengharuskan Anda untuk menyetujui Syarat dan Ketentuan sebelum Anda dapat mengunduh dokumen. Setiap unduhan dokumen memiliki watermark unik yang dapat dilacak.

Anda hanya diizinkan untuk berbagi dokumen yang ditandai sebagai dokumen rahasia dengan lingkaran dalam perusahaan Anda, dengan regulator Anda, dan dengan auditor Anda. Anda tidak diizinkan untuk berbagi dokumen ini dengan pelanggan Anda atau di situs web Anda. Kami sangat menyarankan agar Anda menggunakan layanan berbagi dokumen yang aman, seperti Amazon WorkDocs, untuk berbagi

dokumen dengan orang lain. Jangan mengirim dokumen melalui email atau mengunggahnya ke situs yang tidak aman.

Pemecahan Masalah

Jika Anda tidak dapat mengunduh dokumen atau menerima pesan kesalahan, lihat Pemecahan Masalah di FAQ AWS Artifact.

Mengelola perjanjian di AWS Artifact

Perjanjian AWS Artifact memungkinkan Anda menggunakan AWS Management Console untuk meninjau, menerima, dan mengelola perjanjian untuk akun atau organisasi Anda. Misalnya, Perjanjian Rekanan Bisnis (BAA) biasanya diperlukan untuk perusahaan yang tunduk pada Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) untuk memastikan bahwa informasi kesehatan yang dilindungi (PHI) dijaga dengan benar. Anda dapat menggunakan AWS Artifact untuk menerima perjanjian seperti BAA dengan AWS, dan menunjuk satu akun AWS yang secara legal dapat memproses PHI. Jika menggunakan AWS Organizations, Anda dapat menerima perjanjian seperti BAA AWS atas nama semua akun dalam organisasi Anda. Semua akun anggota yang ada dan selanjutnya secara otomatis tercakup dalam perjanjian dan dapat memproses PHI secara legal.

Anda juga dapat menggunakan AWS Artifact untuk mengonfirmasi bahwa akun AWS atau organisasi Anda menerima sebuah perjanjian dan untuk meninjau persyaratan perjanjian yang diterima guna memahami kewajiban Anda. Jika akun atau organisasi Anda tidak lagi perlu menggunakan perjanjian yang diterima tersebut, Anda dapat menggunakan AWS Artifact untuk mengakhiri perjanjian. Jika Anda mengakhiri perjanjian tetapi kemudian menyadari bahwa Anda membutuhkannya, Anda dapat mengaktifkannya lagi.

Daftar Isi

Mengelola perjanjian untuk satu akun di AWS Artifact

Anda dapat menerima perjanjian hanya untuk akun Anda, meskipun akun Anda adalah akun anggota dalam organisasi di AWS Organizations. Untuk informasi selengkapnya tentang AWS Organizations, lihat Panduan Pengguna AWS Organizations.

Menerima perjanjian dengan AWS

Sebelum Anda menerima perjanjian, sebaiknya Anda berkonsultasi dengan tim legal, privasi, dan kepatuhan Anda.

Izin yang diperlukan

Jika Anda adalah administrator akun, Anda dapat memberikan izin kepada pengguna IAM dan pengguna gabungan untuk mengakses dan mengelola satu atau beberapa perjanjian Anda. Secara default, hanya pengguna dengan hak administratif yang dapat menerima perjanjian. Untuk menerima perjanjian, pengguna IAM dan pengguna gabungan harus memiliki izin berikut:

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

Untuk informasi lebih lanjut, lihat Identity and access management (p. 10).

Untuk menerima perjanjian dengan AWS

1. Buka konsol AWS Artifact pada https://console.aws.amazon.com/artifact/.

2. Pada panel navigasi AWS Artifact, pilih Perjanjian.
3. Pilih tab Perjanjian akun.
4. Perluas bagian perjanjian.
5. Pilih Unduh dan tinjau.
6. Baca Syarat dan Ketentuan. Setelah selesai, pilih Terima dan unduh.
7. Tinjau perjanjian, kemudian pilih kotak centang untuk menunjukkan bahwa Anda setuju.
8. Pilih Terima untuk menerima perjanjian untuk akun Anda.

Mengakhiri perjanjian dengan AWS

Jika Anda menggunakan konsol AWS Artifact untuk menerima perjanjian, Anda dapat menggunakan konsol untuk mengakhiri perjanjian itu. Jika tidak menggunakan konsol, lihat Perjanjian offline (p. 9).

Izin yang diperlukan

Untuk mengakhiri perjanjian, pengguna IAM dan pengguna gabungan harus memiliki izin berikut:

```
artifact:TerminateAgreement
```

Untuk informasi lebih lanjut, lihat Identity and access management (p. 10).

Untuk mengakhiri perjanjian online Anda dengan AWS

1. Buka konsol AWS Artifact pada https://console.aws.amazon.com/artifact/.
2. Pada panel navigasi AWS Artifact, pilih Perjanjian.
3. Pilih tab Perjanjian akun.
4. Pilih perjanjian dan pilih Akhiri perjanjian.
5. Pilih semua kotak centang untuk menunjukkan bahwa Anda setuju untuk mengakhiri perjanjian.
6. Pilih Akhiri. Ketika diminta konfirmasi, pilih Akhiri.

Mengelola perjanjian untuk beberapa akun di AWS Artifact

Jika akun Anda adalah pemilik akun manajemen di organisasi AWS Organizations, Anda dapat menggunakan menerima sebuah perjanjian atas nama semua akun dalam organisasi Anda. Anda harus masuk ke akun manajemen dengan izin AWS Artifact yang tepat untuk menerima atau mengakhiri perjanjian organisasi. Pengguna akun anggota dengan izin `describeOrganizations` dapat melihat perjanjian organisasi yang diterima atas nama mereka.

Jika akun Anda bukan bagian dari organisasi, Anda dapat membuat atau bergabung dengan organisasi dengan mengikuti petunjuk di bagian Membuat dan mengelola organisasi dalam Panduan Pengguna AWS Organizations.

AWS Organizations memiliki dua set fitur yang tersedia: fitur tagihan terkonsolidasi dan semua fitur. Untuk menggunakan AWS Artifact bagi organisasi, organisasi yang menaungi Anda harus diizinkan untuk mengaktifkan semua fitur. Jika organisasi Anda dikonfigurasi hanya untuk tagihan terkonsolidasi, lihat Mengaktifkan semua fitur di organisasi Anda dalam Panduan Pengguna AWS Organizations.

Jika akun anggota dihapus dari organisasi, maka akun anggota tersebut tidak akan lagi tercakup oleh perjanjian organisasi. Administrator akun pengelolaan harus menyampaikan hal ini ke akun anggota

sebelum menghapus akun anggota dari organisasi, sehingga akun anggota dapat menempatkan perjanjian baru jika diperlukan. Daftar perjanjian organisasi aktif dapat dilihat di Perjanjian organisasi AWS Artifact.

Untuk informasi selengkapnya, lihat Mengelola akun AWS di organisasi Anda dalam Panduan Pengguna AWS Organizations.

Menerima perjanjian untuk organisasi Anda

Anda dapat menerima perjanjian atas nama semua akun anggota dalam organisasi Anda di AWS Organizations. Sebelum Anda menerima perjanjian, sebaiknya Anda berkonsultasi dengan tim legal, privasi, dan kepatuhan Anda.

Izin yang diperlukan

Untuk menerima perjanjian, pemilik akun manajemen harus memiliki izin berikut:

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

Untuk informasi lebih lanjut, lihat Identity and access management (p. 10).

Untuk menerima perjanjian bagi organisasi

1. Buka konsol AWS Artifact pada https://console.aws.amazon.com/artifact/.
2. Pada dasbor AWS Artifact, pilih Perjanjian.
3. Pilih tab Perjanjian organisasi.
4. Perluas bagian perjanjian.
5. Pilih Unduh dan tinjau.
6. Baca Syarat dan Ketentuan. Setelah selesai, pilih Terima dan unduh.
7. Tinjau perjanjian, kemudian pilih kotak centang untuk menunjukkan bahwa Anda setuju.
8. Pilih Terima untuk menerima perjanjian untuk semua akun yang ada dan yang akan datang di organisasi Anda..

Mengakhiri perjanjian organisasi

Jika Anda menggunakan konsol AWS Artifact untuk menerima perjanjian atas nama semua akun anggota dalam organisasi, Anda dapat menggunakan konsol tersebut untuk mengakhiri perjanjian itu. Jika tidak menggunakan konsol, lihat Perjanjian offline (p. 9).

Izin yang diperlukan

Untuk mengakhiri perjanjian, pemilik akun manajemen harus memiliki izin berikut:

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

```
iam:CreateRole
iam:AttachRolePolicy
```

Untuk informasi lebih lanjut, lihat Identity and access management (p. 10).

Untuk mengakhiri perjanjian organisasi online Anda dengan AWS

1. Buka konsol AWS Artifact pada https://console.aws.amazon.com/artifact/.
2. Pada dasbor AWS Artifact, pilih Perjanjian.
3. Pilih tab Perjanjian organisasi.
4. Pilih perjanjian dan pilih Akhiri perjanjian.
5. Pilih semua kotak centang untuk menunjukkan bahwa Anda setuju untuk mengakhiri perjanjian.
6. Pilih Akhiri. Ketika diminta konfirmasi, pilih Akhiri.

Mengelola perjanjian offline yang ada di AWS Artifact

Jika Anda sudah memiliki perjanjian offline, AWS Artifact menampilkan perjanjian yang Anda terima secara offline. Sebagai contoh, konsol mungkin menampilkan Perjanjian Rekanan Bisnis (BAA) Offline dengan status Aktif. Status aktif menunjukkan bahwa perjanjian tersebut telah diterima. Untuk mengakhiri perjanjian offline, lihat pedoman pengakhiran dan instruksi yang disertakan dalam perjanjian Anda.

Jika akun Anda adalah akun manajemen di organisasi AWS Organizations, Anda dapat menggunakan AWS Artifact untuk menerapkan persyaratan perjanjian offline Anda ke semua akun di organisasi Anda. Untuk menerapkan perjanjian yang diterima secara offline ke organisasi dan semua akun di organisasi Anda, Anda harus memiliki izin berikut:

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

Jika akun Anda adalah akun anggota dalam organisasi, Anda harus memiliki izin berikut untuk melihat perjanjian organisasi offline Anda:

```
organizations:DescribeOrganization
```

Untuk informasi lebih lanjut, lihat Identity and access management (p. 10).

Identity and access management di AWS Artifact

Ketika mendaftar ke AWS, Anda memberikan alamat email dan kata sandi yang terkait dengan akun AWS Anda. Ini adalah kredensial root Anda yang memberikan akses penuh ke semua sumber daya AWS Anda, termasuk sumber daya untuk AWS Artifact. Namun, kami sangat menyarankan agar Anda tidak menggunakan akun root untuk akses sehari-hari. Kami juga menyarankan agar Anda tidak membagikan kredensial akun dengan orang lain untuk memberikan akses penuh ke akun Anda.

Alih-alih masuk ke akun AWS dengan kredensial root atau berbagi kredensial Anda dengan orang lain, Anda sebaiknya membuat identitas pengguna khusus yang disebut pengguna IAM untuk diri sendiri dan siapa saja yang mungkin membutuhkan akses ke dokumen atau perjanjian dalam AWS Artifact. Dengan pendekatan ini, Anda dapat memberikan informasi masuk berbeda untuk setiap pengguna, dan Anda dapat memberikan izin yang dibutuhkan tiap-tiap pengguna untuk bekerja dengan dokumen tertentu saja. Anda juga dapat memberikan izin yang sama kepada beberapa pengguna IAM dengan memberikan izin bagi grup IAM dan menambahkan pengguna IAM ke grup tersebut.

Jika Anda sudah mengelola identitas pengguna di luar AWS, Anda dapat menggunakan penyedia identitas IAM alih-alih membuat pengguna IAM. Untuk informasi selengkapnya, lihat Penyedia dan federasi identitas dalam Panduan Pengguna IAM.

Buat pengguna IAM dan beri mereka akses ke AWS Artifact

Selesaikan langkah-langkah berikut untuk memberikan izin ke AWS Artifact bagi pengguna berdasarkan tingkat akses yang mereka butuhkan.

Tugas

- Langkah 1: Membuat kebijakan IAM (p. 10)
- Langkah 2: Buat grup IAM dan lampirkan kebijakan (p. 11)
- Langkah 3: Buat pengguna IAM dan tambahkan ke grup (p. 11)

Langkah 1: Membuat kebijakan IAM

Sebagai administrator IAM, Anda dapat membuat kebijakan yang memberikan izin untuk tindakan dan sumber daya AWS Artifact.

Untuk membuat kebijakan IAM

Gunakan prosedur berikut untuk membuat kebijakan IAM yang dapat Anda gunakan untuk memberikan izin kepada pengguna dan grup IAM.

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.

4. Pilih tab JSON.
5. Masukkan dokumen kebijakan. Anda dapat membuat kebijakan sendiri, atau Anda dapat menggunakan salah satu kebijakan dari Kebijakan contoh IAM (p. 11).
6. Pilih Tinjau Kebijakan. Validator kebijakan melaporkan kesalahan sintaksis.
7. Pada halaman Tinjau kebijakan, masukkan nama unik yang membantu Anda mengingat tujuan kebijakan. Anda juga dapat menambahkan deskripsi.
8. Pilih Buat kebijakan.

Langkah 2: Buat grup IAM dan lampirkan kebijakan

Sebagai administrator IAM, Anda dapat membuat grup dan melampirkan kebijakan yang Anda buat ke grup. Anda dapat menambahkan pengguna IAM ke grup kapan saja.

Untuk membuat grup IAM dan melampirkan kebijakan

1. Dalam panel navigasi, pilih Groups lalu pilih Create New Group.
2. Untuk Nama Grup, masukkan nama untuk grup Anda, lalu pilih Langkah Selanjutnya.
3. Di bidang pencarian, masukkan nama kebijakan yang Anda buat. Pilih kotak centang untuk kebijakan Anda, kemudian pilih Langkah Selanjutnya.
4. Tinjau nama grup dan kebijakan. Setelah semuanya selesai, pilih Buat Grup.

Langkah 3: Buat pengguna IAM dan tambahkan ke grup

Sebagai administrator IAM, Anda dapat menambahkan pengguna ke grup kapan saja. Ini memberikan kepada pengguna izin yang sama yang diberikan ke grup.

Untuk membuat pengguna IAM dan menambahkannya ke grup

1. Di panel navigasi, pilih Pengguna lalu pilih Tambahkan pengguna.
2. Untuk Nama pengguna, masukkan nama untuk satu atau lebih pengguna.
3. Pilih kotak centang di samping akses AWS Management Console. Konfigurasikan sandi yang dibuat secara otomatis atau kustom. Anda dapat memilih Pengguna harus membuat kata sandi baru saat masuk berikutnya untuk mengharuskan pengguna mengatur ulang kata sandi baru saat masuk pertama kali.
4. Pilih Berikutnya: Izin.
5. Pilih Tambahkan pengguna ke grup lalu pilih grup yang Anda buat.
6. Pilih Berikutnya: Tanda. Anda dapat menambahkan tag secara opsional ke pengguna Anda.
7. Pilih Berikutnya: Peninjauan. Setelah semuanya selesai, pilih Buat pengguna.

Kebijakan contoh IAM

Anda dapat membuat kebijakan izin yang memberikan izin kepada pengguna IAM. Anda dapat memberikan akses bagi pengguna ke laporan AWS Artifact dan kemampuan untuk menerima dan mengunduh perjanjian atas nama satu akun atau organisasi.

Contoh kebijakan berikut menunjukkan izin yang dapat Anda tetapkan untuk pengguna IAM berdasarkan tingkat akses yang mereka butuhkan.

Example Contoh kebijakan untuk mengelola laporan

Kebijakan berikut memberikan izin untuk mengunduh semua laporan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "artifact:Get"
            ],
            "Resource": [
                "arn:aws:artifact:::report-package/*"
            ]
        }
    ]
}
```

Kebijakan berikut memberikan izin untuk mengunduh hanya laporan SOC, PCI, dan ISO.

```
{
    "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 Contoh kebijakan untuk mengelola perjanjian

Kebijakan berikut memberikan izin untuk mengunduh semua perjanjian. Pengguna IAM juga harus memiliki izin ini untuk menerima perjanjian.

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

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

Kebijakan berikut memberikan izin untuk menerima perjanjian.

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

Kebijakan berikut memberikan izin untuk mengakhiri perjanjian.

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

Kebijakan berikut memberikan izin untuk mengelola perjanjian satu akun.

```
{
    "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 Contoh kebijakan untuk diintegrasikan dengan AWS Organizations

Kebijakan berikut memberikan izin untuk membuat IAM role yang digunakan AWS Artifactuntuk diintegrasikan dengan AWS Organizations. Akun manajemen organisasi Anda harus memiliki izin ini untuk memulai perjanjian organisasi.

```
{
    "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"
                }
            }
        }
    ]
}
```

Kebijakan berikut memberikan izin untuk memberikan izin kepada AWS Artifact untuk menggunakan AWS Organizations. Akun manajemen organisasi Anda harus memiliki izin ini untuk memulai perjanjian organisasi.

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

Example Contoh kebijakan untuk mengelola perjanjian bagi akun manajemen

Kebijakan berikut memberikan izin untuk mengelola perjanjian bagi akun manajemen.

```
{
    "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 Contoh kebijakan untuk mengelola perjanjian organisasi

Kebijakan berikut memberikan izin untuk mengelola perjanjian organisasi. Pengguna lain dengan izin yang diperlukan harus menyiapkan perjanjian organisasi.

```
{
    "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": "*"
        }
    ]
}
```

Kebijakan berikut memberikan izin untuk melihat perjanjian organisasi.

```
{
    "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": "*"
        }
    ]
}
```

Cross-service bingung wakil pencegahan

Masalah deputi yang bingung adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan tersebut. MasukAWS, peniruan lintas layanan dapat mengakibatkan masalah wakil bingung. Peniruan lintas layanan dapat terjadi ketika satu layanan (panggilanlayanan) panggilan layanan lain (disebutlayanan). Layanan panggilan dapat dimanipulasi untuk menggunakan izin untuk bertindak atas sumber daya pelanggan lain dengan cara yang seharusnya tidak memiliki izin untuk mengakses. Untuk mencegah hal ini,AWSmenyediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsipal layanan yang telah diberikan akses ke sumber daya di akun Anda.

Bila Anda mengaktifkan akses terpercaya antaraAWS ArtifactdanAWS Organizations, kami secara otomatis membuat peran dengan kebijakan di akun Anda yang membatasi siapa yang dapat menganggap peran tersebut.

Kami menggunakan`aws:SourceArn`dan`aws:SourceAccount`kunci konteks kondisi global dalam kebijakan kepercayaan untuk membatasi entitas yang dapat mengasumsikan peran layanan yang kami buat di akun Anda. Dengan kunci konteks kondisi global,`aws:SourceAccount`nilai dan akun di`aws:SourceArn`nilai harus menggunakan ID akun yang sama bila digunakan dalam pernyataan kebijakan yang sama.

Di bawah ini adalah contoh kebijakan yang kami buat dengan peran saat Anda mengaktifkan akses tepercaya antaraAWS ArtifactdanAWS 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"
                }
            }
        }
    ]
}
```

Riwayat dokumen untuk AWS Artifact

Tabel berikut menguraikan rilis untuk AWS Artifact.

perubahan-riwayat-pembaruan	pembaruan-riwayat-deskripsi	pembaruan-riwayat-tanggal
Keamanan (p. 18)	Ditambahkan bagian untuk Identitas dan akses halaman manajemen untuk bingung wakil pencegahan.	Jumat, 20 Desember 2021
Laporan (p. 18)	Menghapus perjanjian kerahasiaan serta memperkenalkan syarat dan ketentuan untuk pengunduhan laporan.	17 Desember 2020
Halaman beranda dan pencarian (p. 18)	Menambahkan halaman beranda layanan dan bilah pencarian pada halaman laporan dan perjanjian.	15 Mei 2020
Peluncuran GovCloud (p. 18)	Meluncurkan AWS Artifact di wilayah GovCloud.	7 November 2019
AWS Organizationsperjanjian (p. 18)	Menambahkan dukungan untuk mengelola perjanjian untuk organisasi.	20 Juni 2018
Perjanjian (p. 18)	Menambahkan dukungan untuk mengelola perjanjian AWS Artifact.	17 Juni 2017
Rilis awal (p. 18)	Rilis ini memperkenalkan AWS Artifact.	Selasa, 30 Nopember 2016

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.