User Guide

AWS Artifact

AWS Artifact: User Guide

Table of Contents

Was ist AWS Artifact?

AWS Artifactbietet On-Demand-Downloads vonAWS Sicherheits- und Compliance-Dokumenten wieAWS ISO-Zertifizierungen, PCI-Berichten (Payment Card Industry) und Service Organization Control (SOC) -Berichten. Sie können die Sicherheits- und Compliance-Dokumente (auch als Prüfungswerkzeuge bezeichnet) an die Prüfer oder Regulierungsbehörden senden, um die Sicherheit und Compliance der von Ihnen genutzten AWS-Infrastruktur und -Services nachzuweisen. Sie können diese Dokumente auch als Richtlinien verwenden, um Ihre eigene Cloud-Architektur zu bewerten und die Wirksamkeit der internen Kontrollen Ihres Unternehmens zu bewerten.

Darüber hinausAWS Artifact bietet es auf Abruf die Sicherheits- und Compliance-Dokumente wie ISO-Zertifizierungen und SOC-Berichte (Service Organization Control) der unabhängigen Softwareanbieter (ISVs), die ihre Produkte verkaufen, zum HerunterladenAWS Marketplace. Weitere Informationen finden Sie unter Finden von AWS Marketplace-Vendor Insights.

AWSKunden sind dafür verantwortlich, Dokumente zu erstellen oder zu beschaffen, die die Sicherheit und Konformität ihrer Unternehmen belegen. Weitere Informationen finden Sie unter Modell der gemeinsamen Verantwortung.

Sie können AWS Artifact auch für das Überprüfen, Akzeptieren und Nachverfolgen des Status von AWS-Vereinbarungen wie unserem Business Associate Addendum (BAA) verwenden. Eine BAA ist in der Regel für Unternehmen erforderlich, die dem Health Insurance Portability and Accountability Act (HIPAA) unterliegen, um sicherzustellen, dass geschützte Gesundheitsinformationen (PHI) angemessen geschützt sind. Mit AWS Artifact können Sie Vereinbarungen mit AWS akzeptieren und AWS-Konten zuweisen, die vertrauliche Informationen verarbeiten dürfen. Sie können eine Vereinbarung für mehrere Konten akzeptieren. Verwenden Sie AWS Organizations zum Erstellen einer Organisation, um Vereinbarungen für mehrere Konten zu akzeptieren.

Weitere Informationen finden Sie unter AWS Artifact.

Preise

AWSstellt IhnenAWS Artifact Dokumente und Vereinbarungen kostenlos zur Verfügung.

Erste Schritte mit AWS Artifact

AWS Artifact bietet eine zentrale Ressource für AWS Sicherheits- und Compliance-Berichte. Die Artefakte sind verfügbar in AWS Artifact Dazu gehören Berichte zur Kontrolle der Serviceorganisation (SOC), Berichte über die Zahlungskartenbranche (PCI) und Zertifizierungen von Akkreditierungsstellen, die die Implementierung und Betriebseffizienz von AWS Sicherheitskontrollen. Zusätzlich AWS Artifact bietet auf Abruf Zugriff auf die Sicherheits- und Compliance-Dokumente wie ISO Zertifizierungen und Service Organization Control (SOC) -Berichte der unabhängigen Softwareanbieter (ISVs), die ihre Produkte verkaufen AWS Marketplace Weitere Informationen finden Sie unter .AWS Marketplace Einblicke in Anbieter.

AWS Artifact ermöglicht es Ihnen, rechtliche Vereinbarungen wie den Business Associate Addendum () BAA zu akzeptieren und zu verwalten. Wenn Sie verwenden AWS Organizations, können Sie Vereinbarungen im Namen aller Konten innerhalb Ihrer Organisation akzeptieren. Anschließend fallen alle vorhandenen und folgenden Mitgliedskonten automatisch unter die akzeptierte Vereinbarung.

Aufgaben

- Schritt 1: Melden Sie sich an für AWS
- Schritt 2: Laden Sie einen Bericht herunter
- Schritt 3: Verträge verwalten
- Schritt 4: Benachrichtigungen verwalten

Schritt 1: Melden Sie sich an für AWS

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, ein Root-Benutzer des AWS-Kontoswird erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen im Konto. Als bewährte

Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Schritt 2: Laden Sie einen Bericht herunter

Sie können Berichte mit dem Adobe Acrobat Reader herunterladen. Andere PDF Reader werden nicht unterstützt. Weitere Informationen finden Sie unter Berichte werden heruntergeladen.

So laden Sie einen Bericht herunter

1. Öffnen Sie AWS Artifact Konsole bei https://console.aws.amazon.com/artifact/.
2. Auf der AWS Artifact Wählen Sie auf der Startseite Berichte anzeigen aus.
3. Verwenden Sie auf der Seite Berichte die AWS Auf die Registerkarte „Berichte“ können Sie zugreifen AWS Berichte (z. B. SOC 1/2/3PCI, C5 usw.) und navigieren Sie zur Registerkarte Berichte von Drittanbietern, um auf die Berichte der unabhängigen Softwareanbieter (ISVs) zuzugreifen, über die sie ihre Produkte verkaufen AWS Marketplace.
4. (Optional) Geben Sie ein Schlüsselwort in das Suchfeld ein, um nach einem Bericht zu suchen. Sie können anhand einzelner Spalten, einschließlich Berichtstitel, Kategorie, Serie und Beschreibung, gezielt nach Berichten suchen. Wenn Sie beispielsweise den Bericht „Cloud Computing Compliance Controls Catalogue“ (C5) suchen müssen, können Sie die Spalte „Titel“ mit dem Operator „enthält“ und dem Begriff „C5“ durchsuchen.
5. Wählen Sie einen Bericht aus und klicken Sie dann auf Bericht herunterladen.
6. (Optional) Auf der Registerkarte Berichte von Drittanbietern können Sie auf die Detailseite eines ISV Berichts zugreifen, indem Sie auf den Berichtstitel klicken, um mehr über den Bericht zu erfahren.
7. Möglicherweise werden Sie aufgefordert, die Allgemeinen Geschäftsbedingungen zu akzeptieren, die für den jeweiligen Bericht gelten, den Sie herunterladen. Wir empfehlen Ihnen, diese aufmerksam zu lesen. Wenn Sie fertig sind, wählen Sie Ich habe die Nutzungsbedingungen gelesen und stimme ihnen zu und wählen Sie dann Nutzungsbedingungen akzeptieren und Bericht herunterladen aus.
8. Öffnen Sie die heruntergeladene Datei über einen PDF Viewer. Lesen Sie die Annahmebedingungen und scrollen Sie nach unten, um den Prüfbericht zu finden. Berichte können zusätzliche Informationen als Anlagen in das PDF Dokument eingebettet haben. Achten

Sie daher darauf, in der PDF Datei nach Anhängen zu suchen, um unterstützende Dokumente zu erhalten. Anweisungen zum Anzeigen von Anhängen finden Sie hier.

Berichte von Drittanbietern sind nur zugänglich für AWS Kunden, die sich angemeldet haben bei AWS Marketplace Einblicke in Lieferanten. Weitere Informationen hierzu finden Sie unter .AWS Marketplace Einblicke von Anbietern.

Schritt 3: Verträge verwalten

Bevor Sie eine Vereinbarung abschließen, müssen Sie die Bedingungen des herunterladen und ihnen zustimmen AWS Artifact Geheimhaltungsvereinbarung (NDA). Jede Vereinbarung ist vertraulich und kann nicht an Dritte außerhalb Ihres Unternehmens weitergegeben werden.

Um eine Vereinbarung zu akzeptieren mit AWS

1. Öffnen Sie AWS Artifact Konsole bei https://console.aws.amazon.com/artifact/.
2. Auf der AWS Artifact Wählen Sie im Navigationsbereich Vereinbarungen aus.
3. Wählen Sie Kontovereinbarungen, um Vereinbarungen für Ihr Konto zu verwalten, oder Organisationsvereinbarungen, um Vereinbarungen im Namen Ihrer Organisation zu verwalten.
4. Erweitern Sie den Abschnitt der Vereinbarung.
5. Wählen Sie Herunterladen und überprüfen.
6. Lesen Sie die Allgemeinen Geschäftsbedingungen. Wenn Sie fertig sind, wählen Sie Akzeptieren und herunterladen.
7. Überprüfen Sie die Vereinbarung und aktivieren Sie dann die Kontrollkästchen, um anzugeben, dass Sie damit einverstanden sind.
8. Wählen Sie Annehmen, um die Vereinbarung zu akzeptieren.

Weitere Informationen finden Sie unter Verwaltung von Vereinbarungen.

Schritt 4: Benachrichtigungen verwalten

Sie können Benachrichtigungen über die Verfügbarkeit neuer Berichte und Vereinbarungen oder über Aktualisierungen vorhandener Berichte und Vereinbarungen abonnieren. AWSArtifact verwendet den AWS Benutzerbenachrichtigungsdienst, um Benachrichtigungen zu senden.

Benachrichtigungen werden an E-Mail-Adressen gesendet, die der Benutzer bei der Einrichtung der Benachrichtigungskonfiguration angibt.

Um eine Konfiguration zu erstellen

1. Öffnen Sie die Seite mit den Benachrichtigungs-Hubs im Dienst AWS für Benutzerbenachrichtigungen
2. Wählen Sie die Region (en) aus, in denen Sie Ihre Ressourcen für AWS Benutzerbenachrichtigungen speichern möchten. Standardmäßig werden Ihre Benutzerbenachrichtigungsdaten in USA Ost (Nord-Virginia) gespeichert und in anderen von Ihnen ausgewählten Regionen repliziert. Weitere Informationen finden Sie in der Dokumentation zu Notification Hubs.
3. Klicken Sie auf Konfiguration erstellen.
4. Um Benachrichtigungen über Vereinbarungen zu erhalten, klicken Sie auf das Kontrollkästchen für Aktualisierungen zu AWS Vereinbarungen.
5. Um Benachrichtigungen für Berichte zu erhalten, klicken Sie auf das Kontrollkästchen für Aktualisierungen zu AWS Berichten. Um nur Benachrichtigungen für Berichte zu bestimmten Kategorien und Serien zu erhalten, klicken Sie auf das Kontrollkästchen für Eine Untergruppe von Berichten und dann auf das Kontrollkästchen für die Kategorien und Serien, an denen Sie interessiert sind.
6. Geben Sie einen Namen für Ihre Konfiguration ein.
7. Geben Sie eine durch Kommas getrennte Liste von E-Mails ein, an die Benachrichtigungen gesendet werden sollen.
8. (Optional) Um der Benachrichtigungskonfiguration ein Tag zuzuweisen, geben Sie die Schlüssel-Wert-Paare ein, indem Sie den Abschnitt Tags erweitern. Hinweis: Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen können. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, den Sie definieren können. Mithilfe von Tags können Sie Ressourcen verwalten, suchen und filtern.
9. Klicken Sie auf Submit.
10. Eine Bestätigungs-E-Mail wird an die angegebenen E-Mail-Adressen gesendet und die E-Mail-Empfänger müssen in der an sie gesendeten Bestätigungs-E-Mail auf den Link E-Mail verifizieren klicken. Bitte beachten Sie, dass nur verifizierte E-Mail-Adressen Benachrichtigungen erhalten.

Weitere Informationen finden Sie unter Benachrichtigungen verwalten.

Berichte werden heruntergeladen in AWS Artifact

Sie können Berichte von der AWS Artifact Konsole herunterladen. Wenn Sie einen Bericht von herunterladen AWS Artifact, wird der Bericht speziell für Sie generiert, und jeder Bericht hat ein eindeutiges Wasserzeichen. Aus diesem Grund sollten Sie die Berichte nur für Personen freigeben, denen Sie vertrauen. Versenden Sie die Berichte nicht als E-Mail-Anhang und geben Sie sie nicht online frei. Verwenden Sie einen sicheren Sharing-Dienst wie Amazon, um einen Bericht zu teilen WorkDocs. Bei einigen Berichten müssen Sie die Allgemeinen Geschäftsbedingungen akzeptieren, bevor Sie sie herunterladen können.

Inhalt

Einen Bericht wird heruntergeladen

Um einen Bericht herunterzuladen, benötigen Sie die erforderlichen Berechtigungen. Weitere Informationen finden Sie unter Identity and Access Management in AWS Artifact.

Wenn Sie sich für registrieren AWS Artifact, erhält Ihr Konto automatisch die Erlaubnis, einige Berichte herunterzuladen. Wenn Sie Probleme beim Zugriff haben AWS Artifact, folgen Sie den Anweisungen auf der Seite AWS Artifact Service Authorization Reference.

So laden Sie einen Bericht herunter

1. Öffnen Sie die AWS Artifact Konsole unter https://console.aws.amazon.com/artifact/.
2. Wählen Sie auf der AWS Artifact Startseite Berichte anzeigen aus.
3. Verwenden Sie auf der Seite Berichte die Registerkarte AWS Berichte, um auf AWS Berichte zuzugreifen (z. B. SOC 1/2/3,PCI, C5 usw.), und navigieren Sie zur Registerkarte Berichte von Drittanbietern, um auf die Berichte der unabhängigen Softwareanbieter (ISVs) zuzugreifen, über die ihre Produkte verkauft werden. AWS Marketplace
4. (Optional) Geben Sie ein Schlüsselwort in das Suchfeld ein, um nach einem Bericht zu suchen. Sie können anhand einzelner Spalten, einschließlich Berichtstitel, Kategorie, Serie und

Beschreibung, gezielt nach Berichten suchen. Wenn Sie beispielsweise den Bericht „Cloud Computing Compliance Controls Catalogue“ (C5) suchen müssen, können Sie die Spalte „Titel“ mit dem Operator „enthält“ und dem Begriff „C5“ durchsuchen.

5. Wählen Sie einen Bericht aus und klicken Sie dann auf Bericht herunterladen.
6. (Optional) Auf der Registerkarte Berichte von Drittanbietern können Sie auf die Detailseite eines ISV Berichts zugreifen, indem Sie auf den Berichtstitel klicken, um mehr über den Bericht zu erfahren.
7. Möglicherweise werden Sie aufgefordert, die Allgemeinen Geschäftsbedingungen zu akzeptieren, die für den jeweiligen Bericht gelten, den Sie herunterladen. Wir empfehlen Ihnen, diese aufmerksam zu lesen. Wenn Sie fertig sind, wählen Sie Ich habe die Nutzungsbedingungen gelesen und stimme ihnen zu und wählen Sie dann Nutzungsbedingungen akzeptieren und Bericht herunterladen aus.
8. Öffnen Sie die heruntergeladene Datei über einen PDF Viewer. Lesen Sie die Annahmebedingungen und scrollen Sie nach unten, um den Prüfbericht zu finden. Berichte können zusätzliche Informationen enthalten, die als Anlagen in das PDF Dokument eingebettet sind. Achten Sie daher darauf, in der PDF Datei nach Anhängen zu suchen, um unterstützende Dokumente zu erhalten. Anweisungen zum Anzeigen von Anhängen finden Sie hier.

Anlagen in PDF Dokumenten anzeigen

Die folgenden Anwendungen, die derzeit das Anzeigen von PDF Anhängen unterstützen, werden empfohlen:

Adobe Acrobat Viewer

1. Laden Sie die neueste Version von Adobe Acrobat von hier herunter.
2. Öffnen Sie die Datei im Adobe Acrobat Viewer.
3. Um das Anlagenfenster zu öffnen, klicken Sie links im PDF Dokument auf das Büroklammersymbol oder wählen Sie „Ansicht“ > „Ein-/Ausblenden“ > „Navigationsfenster“ > „Anlagen“.
4. Doppelklicken Sie im Fenster „Anlagen“ auf die Anlage, um das Dokument anzuzeigen.

Firefox-Browser

1. Laden Sie den Firefox-Browser von hier herunter

2. Öffnen Sie die PDF Datei im Firefox-Browser, indem Sie die Option Datei öffnen im Menü Datei verwenden.
3. Um die Anlagen zu öffnen, klicken Sie oben links auf dem Bildschirm auf das Symbol „Seitenleiste umschalten“.

Sicherung Ihrer Dokumente

AWS Artifact Dokumente sind vertraulich und sollten jederzeit sicher aufbewahrt werden. AWS Artifact verwendet für seine Dokumente das Modell der AWS gemeinsamen Verantwortung. Das bedeutet, dass AWS es für die Sicherheit von Dokumenten verantwortlich ist, solange sie sich in der AWS Cloud befinden, aber Sie sind dafür verantwortlich, sie nach dem Herunterladen zu schützen. AWS Artifact Möglicherweise müssen Sie die Allgemeinen Geschäftsbedingungen akzeptieren, bevor Sie Dokumente herunterladen können. Jeder Dokument-Download verfügt über ein eindeutiges nachverfolgbares Wasserzeichen.

Sie dürfen Dokumente, die als vertraulich gekennzeichnet sind, nur innerhalb Ihres Unternehmens, mit Ihren Aufsichtsbehörden und Ihren Prüfern teilen. Sie dürfen diese Dokumente nicht an Kunden weitergeben oder auf Ihrer Website veröffentlichen. Wir empfehlen Ihnen dringend, einen sicheren Dienst für die gemeinsame Nutzung von Dokumenten wie Amazon zu verwenden WorkDocs, um Dokumente mit anderen zu teilen. Senden Sie die Dokumente nicht per E-Mail und laden Sie sie nicht auf eine unsichere Website hoch.

Fehlerbehebung

Wenn Sie ein Dokument nicht herunterladen können oder keine Fehlermeldung erhalten, finden Sie weitere Informationen unter Problembehandlung in der AWS Artifact FAQ.

Verwaltung von Vereinbarungen in AWS Artifact

AWS Artifact-Vereinbarungen ermöglichen die Nutzung von AWS Management Console zum Prüfen, Akzeptieren und Verwalten von Vereinbarungen für Ihr Konto oder Ihre Organisation. Eine Business Associate Addendum-Vereinbarung (BAA) ist in der Regel für Unternehmen erforderlich, die dem Health Insurance Portability and Accountability Act (HIPAA) unterliegen. Sie stellt sicher, dass vertrauliche Gesundheitsinformationen (PHI) angemessen geschützt sind. Mit AWS Artifact können Sie eine Vereinbarung wie z. B. die BAA mit AWS akzeptieren und ein AWS-Konto benennen, das vertrauliche Gesundheitsinformationen verarbeiten darf. Wenn Sie AWS Organizations verwenden, können Sie Vereinbarungen wie die AWS-BAA für alle Konten in Ihrer Organisation akzeptieren. Alle vorhandenen und folgenden Mitgliedskonten fallen automatisch unter die Vereinbarung und dürfen vertrauliche Gesundheitsinformationen verarbeiten.

Sie können mit AWS Artifact auch bestätigen, dass Ihr AWS-Konto oder Ihre Organisation eine Vereinbarung akzeptiert hat, und die Bedingungen der akzeptierten Vereinbarung prüfen, um sich mit Ihren Verpflichtungen vertraut zu machen. Wenn Ihr Konto oder Ihre Organisation die akzeptierte Vereinbarung nicht mehr verwenden muss, können Sie AWS Artifact sie zur Kündigung der Vereinbarung verwenden. Wenn Sie die Vereinbarung kündigen, aber später feststellen, dass Sie sie benötigen, können Sie sie erneut aktivieren.

Inhalt

Verwaltung einer Vereinbarung für ein einzelnes Konto in AWS Artifact

Sie können Vereinbarungen nur für Ihr Konto akzeptieren, auch wenn das Konto ein Mitgliedskonto in einer Organisation in AWS Organizations ist. Weitere Informationen zu AWS Organizations finden Sie im AWS Organizations Benutzerhandbuch.

Annahme einer Vereinbarung mit AWS

Bevor Sie eine Vereinbarung akzeptieren, empfehlen wir Ihnen, Ihr Rechts-, Datenschutz- und Compliance-Team anzusprechen.

Erforderliche Berechtigungen

Wenn Sie Administrator eines Kontos sind, können Sie IAM-Benutzern und Verbundbenutzern mit Rollen die Berechtigungen für den Zugriff und die Verwaltung einer oder mehrerer Ihrer Vereinbarungen gewähren. Standardmäßig können nur Benutzer mit Administratorberechtigungen eine Vereinbarung akzeptieren. Um eine Vereinbarung zu akzeptieren, müssen IAM- und Verbundbenutzer über die folgenden Berechtigungen verfügen:

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

Weitere Informationen finden Sie unter Identity and Access Management.

So akzeptieren Sie eine Vereinbarung mit AWS

1. Öffnen Sie die AWS Artifact Konsole unter https://console.aws.amazon.com/artifact/.
2. Wählen Sie im AWS Artifact-Navigationsbereich die Option Agreements (Vereinbarungen).
3. Wählen Sie die Registerkarte Account agreements (Kontovereinbarungen).
4. Erweitern Sie den Abschnitt der Vereinbarung.
5. Wählen Sie Herunterladen und überprüfen.
6. Lesen Sie die Allgemeinen Geschäftsbedingungen. Wenn Sie fertig sind, wählen Sie Akzeptieren und herunterladen.
7. Überprüfen Sie die Vereinbarung und aktivieren Sie dann die Kontrollkästchen, um anzugeben, dass Sie damit einverstanden sind.
8. Wählen Sie Annehmen, um die Vereinbarung für Ihr Konto zu akzeptieren.

Kündigung einer Vereinbarung mit AWS

Wenn Sie die AWS Artifact-Konsole zum Akzeptieren einer Vereinbarung verwendet haben, können Sie die Konsole auch zum Beenden der Vereinbarung verwenden. Andernfalls lesen Sie unter Offline-Vereinbarungen weiter.

Erforderliche Berechtigungen

Um eine Vereinbarung zu kündigen, müssen IAM- und Verbundbenutzer über die folgenden Berechtigungen verfügen:

```
artifact:TerminateAgreement
```

Weitere Informationen finden Sie unter Identity and Access Management.

So beenden Sie Ihre Online-Vereinbarung mit AWS

1. Öffnen Sie die AWS Artifact Konsole unter https://console.aws.amazon.com/artifact/.
2. Wählen Sie im AWS Artifact-Navigationsbereich die Option Agreements (Vereinbarungen).
3. Wählen Sie die Registerkarte Account agreements (Kontovereinbarungen).
4. Wählen Sie die Vereinbarung aus und klicken Sie auf Vereinbarung kündigen.
5. Markieren Sie alle Kontrollkästchen, um anzugeben, dass Sie mit der Kündigung der Vereinbarung einverstanden sind.
6. Wähen Sie Beenden. Wählen Sie Terminate (Kündigen) aus, wenn Sie zur Bestätigung aufgefordert werden.

Verwaltung einer Vereinbarung für mehrere Konten in AWS Artifact

Wenn Sie der Inhaber des Verwaltungskontos einer AWS Organizations Organisation sind, können Sie eine Vereinbarung im Namen aller Konten in Ihrer Organisation akzeptieren. Sie müssen mit den richtigen AWS Artifact Berechtigungen beim Verwaltungskonto angemeldet sein, um Organisationsvereinbarungen akzeptieren oder kündigen zu können. Benutzer von Hauptkonten mit `organizations:DescribeOrganization`-Berechtigungen können die Organisationsvereinbarungen anzeigen, die Sie für sie akzeptiert haben.

Wenn Ihr Konto nicht Teil einer Organisation ist, können Sie eine Organisation erstellen oder einer Organisation beitreten, indem Sie den Anweisungen unter Organisation erstellen und verwalten im AWS OrganizationsBenutzerhandbuch folgen.

AWS Organizations bietet zwei Funktionsgruppen: Funktionen für die konsolidierte Fakturierung und alle Funktionen. Damit Sie AWS Artifact für Ihre Organisation verwenden können, muss die Organisation, der Sie angehören, für alle Funktionen aktiviert sein. Wenn Ihre Organisation nur für die konsolidierte Fakturierung konfiguriert ist, finden Sie im AWS OrganizationsBenutzerhandbuch weitere Informationen unter Aktivieren aller Funktionen in Ihrer Organisation.

Wenn ein Mitgliedskonto aus einer Organisation entfernt wird, gelten Organisationsvereinbarungen für dieses Konto nicht mehr. Verwaltungskonto-Administratoren sollten Mitgliedskonten

hiervon benachrichtigen, bevor sie die Konten aus der Organisation entfernen, so dass die Mitgliedskonten nötigenfalls neue Vereinbarungen einrichten können. Eine Liste der aktiven Organisationsvereinbarungen kann unter AWS ArtifactOrganisationsvereinbarungen eingesehen werden.

Weitere Informationen finden Sie im AWS OrganizationsBenutzerhandbuch unter Verwaltung der AWS-Konten in Ihrer Organisation.

Annahme einer Vereinbarung für Ihre Organisation

Sie können in AWS Organizations eine Vereinbarung für alle Mitgliedskonten in Ihrer Organisation akzeptieren. Bevor Sie eine Vereinbarung akzeptieren, empfehlen wir Ihnen, Ihr Rechts-, Datenschutz- und Compliance-Team anzusprechen.

Erforderliche Berechtigungen

Um eine Vereinbarung anzunehmen, muss der Besitzer des Verwaltungskontos über die folgenden Berechtigungen verfügen:

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

Weitere Informationen finden Sie unter Identity and Access Management.

So akzeptieren Sie eine Vereinbarung für eine Organisation

1. Öffnen Sie die AWS Artifact Konsole unter https://console.aws.amazon.com/artifact/.
2. Wählen Sie im AWS Artifact-Dashboard die Option Agreements (Vereinbarungen) aus.
3. Wählen Sie die Registerkarte Organization agreements (Organisationsvereinbarungen).
4. Erweitern Sie den Abschnitt der Vereinbarung.
5. Wählen Sie Herunterladen und überprüfen.
6. Lesen Sie die Allgemeinen Geschäftsbedingungen. Wenn Sie fertig sind, wählen Sie Akzeptieren und herunterladen.

7. Überprüfen Sie die Vereinbarung und aktivieren Sie dann die Kontrollkästchen, um anzugeben, dass Sie damit einverstanden sind.
8. Wählen Sie Accept (Akzeptieren), um die Vereinbarung für alle vorhandenen und zukünftigen Konten in Ihrer Organisation zu akzeptieren.

Kündigung einer Organisationsvereinbarung

Wenn Sie die AWS Artifact-Konsole zum Akzeptieren einer Vereinbarung für alle Mitgliedskonten in einer Organisation verwendet haben, können Sie diese Vereinbarung auch über die Konsole beenden. Andernfalls lesen Sie unter Offline-Vereinbarungen weiter.

Erforderliche Berechtigungen

Um eine Vereinbarung zu kündigen, muss der Besitzer des Verwaltungskontos über die folgenden Berechtigungen verfügen:

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

Weitere Informationen finden Sie unter Identity and Access Management.

So beenden Sie Ihre Online-Organisationsvereinbarung mit AWS

1. Öffnen Sie die AWS Artifact Konsole unter https://console.aws.amazon.com/artifact/.
2. Wählen Sie im AWS Artifact-Dashboard die Option Agreements (Vereinbarungen) aus.
3. Wählen Sie die Registerkarte Organization agreements (Organisationsvereinbarungen).
4. Wählen Sie die Vereinbarung aus und klicken Sie auf Vereinbarung kündigen.
5. Markieren Sie alle Kontrollkästchen, um anzugeben, dass Sie mit der Kündigung der Vereinbarung einverstanden sind.
6. Wähen Sie Beenden. Wählen Sie Terminate (Kündigen) aus, wenn Sie zur Bestätigung aufgefordert werden.

Verwaltung einer bestehenden Offline-Vereinbarung in AWS Artifact

Wenn Sie über eine vorhandene Offline-Vereinbarung verfügen, zeigt AWS Artifact die Vereinbarungen an, die Sie offline akzeptiert haben. Die Konsole zeigt beispielsweise Offline Business Associate Addendum (BAA) mit dem Status Active (Aktiv) an. Dieser Status gibt an, dass die Vereinbarung akzeptiert wurde. In den Richtlinien und Anweisungen, die Ihre Vereinbarung zur Beendigung enthält, finden Sie Informationen zum Beenden einer Offline-Vereinbarung.

Wenn Ihr Konto das Verwaltungskonto in einer AWS Organizations Organisation ist, können Sie AWS Artifact damit die Bedingungen Ihrer Offline-Vereinbarung auf alle Konten in Ihrer Organisation anwenden. Wenn Sie eine offline akzeptierte Vereinbarung auf Ihre Organisation und alle Konten in Ihrer Organisation anwenden möchten, benötigen Sie die folgenden Berechtigungen:

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

Wenn Ihr Konto ein Mitgliedskonto in einer Organisation ist, benötigen Sie die folgenden Berechtigungen, um Ihre Offline-Organisationsvereinbarungen anzuzeigen:

```
organizations:DescribeOrganization
```

Weitere Informationen finden Sie unter Identity and Access Management.

Benachrichtigungen verwalten in AWS Artifact

Mit AWS Artifact Notifications können Sie E-Mail-Benachrichtigungen einrichten. Auf der Seite mit den Benachrichtigungseinstellungen können Sie Benachrichtigungen abonnieren und andere Benachrichtigungseinstellungen wie unten beschrieben verwalten. AWS Artifact sendet Benachrichtigungen mithilfe des AWS User Notifications Service. Um AWS Artifact Notifications verwenden zu können, benötigen Sie die erforderlichen Berechtigungen für die Services AWS Artifact und AWS User Notification. Weitere Informationen finden Sie unter Identity and Access Management.

Inhalt

Ihre Benachrichtigungen einrichten

Bevor Sie Benachrichtigungen erhalten können, müssen Sie die Region (en) angeben, in denen Ihre Benutzerbenachrichtigungsdaten gespeichert werden. Gehen Sie wie folgt vor, um Benachrichtigungs-Hubs einzurichten.

So richten Sie Benachrichtigungs-Hubs ein

1. Öffnen Sie die Seite mit den Benachrichtigungs-Hubs im AWS-Dienst für Benutzerbenachrichtigungen.
2. Wählen Sie die Region (en) aus, in denen Sie Ihre AWS-Benutzerbenachrichtigungsressourcen speichern möchten. Standardmäßig werden Ihre Benutzerbenachrichtigungsdaten in USA Ost (Nord-Virginia) gespeichert und in den anderen von Ihnen ausgewählten Regionen repliziert. Weitere Informationen finden Sie in der Dokumentation zu Notification Hubs.
3. Klicken Sie auf Submit.

So abonnieren Sie -Benachrichtigungen

1. Öffnen Sie die Seite mit den Benachrichtigungseinstellungen von AWS Artifact.
2. Klicken Sie auf den Schalter Artifact-Benachrichtigungen abonnieren, um Benachrichtigungen auf AWS Artifact zu abonnieren.

Um Benachrichtigungen abzubestellen

1. Öffnen Sie die Seite mit den Benachrichtigungseinstellungen von AWS Artifact.
2. Klicken Sie auf den Schalter Artifact-Benachrichtigungen abonnieren, um Benachrichtigungen auf AWS Artifact abzubestellen.

Um eine Konfiguration zu erstellen

1. Öffnen Sie die Seite mit den Benachrichtigungseinstellungen von AWS Artifact.
2. Klicken Sie auf Konfiguration erstellen.
3. Um Benachrichtigungen für Vereinbarungen zu erhalten, lassen Sie das Kontrollkästchen neben Updates zu AWS-Verträgen aktiviert.
4. Um Benachrichtigungen für Berichte zu erhalten, lassen Sie das Kontrollkästchen neben Updates on AWS Reports aktiviert.
5. Um Benachrichtigungen für alle Berichte zu erhalten, lassen Sie das Kontrollkästchen neben Alle Berichte aktiviert.
6. Um Benachrichtigungen nur für Berichte zu bestimmten Kategorien und Serien zu erhalten, klicken Sie auf das Kontrollkästchen für Eine Untergruppe von Berichten. Klicken Sie dann auf das Kontrollkästchen für die Kategorien und Serien, an denen Sie interessiert sind.
7. Geben Sie einen Namen für Ihre Konfiguration ein.
8. Geben Sie eine durch Kommas getrennte Liste von E-Mails ein, an die Benachrichtigungen gesendet werden sollen.
9. (Optional) Um der Benachrichtigungskonfiguration ein Tag zuzuweisen, geben Sie die Schlüssel-Wert-Paare ein, indem Sie den Abschnitt Tags erweitern. Hinweis: Ein Tag ist ein Label, das Sie einer AWS-Ressource zuweisen können. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, den Sie definieren können. Mithilfe von Tags können Sie Ressourcen verwalten, suchen und filtern.
10. Klicken Sie auf Konfiguration erstellen.
11. Eine Bestätigungs-E-Mail wird an die angegebenen E-Mail-Adressen gesendet und die E-Mail-Empfänger müssen in der an sie gesendeten Bestätigungs-E-Mail auf den Link E-Mail verifizieren klicken. Bitte beachten Sie, dass nur verifizierte E-Mail-Adressen Benachrichtigungen erhalten.

So bearbeiten eine Konfiguration:

1. Öffnen Sie die Seite mit den Benachrichtigungseinstellungen von AWS Artifact.
2. Klicken Sie auf die Zeile der Konfiguration, die Sie bearbeiten möchten.
3. Klicken Sie oben rechts auf der Seite auf die Schaltfläche Bearbeiten.
4. Sie können jedes der Felder bearbeiten. Wenn Sie mit Ihrer Änderung zufrieden sind, klicken Sie auf Änderungen speichern.
5. Wenn Sie neue E-Mail-Adressen hinzugefügt haben, wird an jede dieser E-Mail-Adressen eine Bestätigungs-E-Mail gesendet. Klicken Sie in der Bestätigungs-E-Mail auf den Link E-Mail verifizieren.

So löschen Sie eine Konfiguration

1. Öffnen Sie die Seite mit den Benachrichtigungseinstellungen von AWS Artifact.
2. Klicken Sie auf die Zeile der Konfiguration, die Sie löschen möchten.
3. Klicken Sie auf Delete.
4. Nachdem Sie die Warnmeldung gelesen haben, klicken Sie auf Löschen.

Einer Konfiguration Tags zuweisen

Ein Tag ist eine Markierung, die Sie einer AWS-Ressource zuordnen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Mithilfe von Tags können Sie Ressourcen verwalten, suchen und filtern. Sie können optional Tags festlegen, wenn Sie eine Konfiguration erstellen oder bearbeiten. Weitere Informationen finden Sie unter Ressourcen taggen

Fehlerbehebung

Wenn Sie bei der Verwendung von AWS Artifact-Benachrichtigungen eine Fehlermeldung erhalten, finden Sie in den AWS Artifact häufig gestellten Fragen weitere Informationen unter Fehlerbehebung.

Identity and Access Management in AWS Artifact

Wenn Sie sich bei AWS anmelden, geben Sie eine mit Ihrem AWS-Konto verknüpfte E-Mail-Adresse und das Passwort ein. Dies sind Ihre Root-Anmeldeinformationen, und sie bieten vollständigen Zugriff auf alle Ihre AWS Ressourcen, einschließlich Ressourcen fürAWS Artifact. Es wird ausdrücklich empfohlen, dass Sie das Root-Konto nicht für den täglichen Zugriff nutzen. Außerdem sollten Sie Anmeldeinformationen nicht gemeinsam mit anderen Personen nutzen, damit diese keinen vollständigen Zugriff auf Ihr Konto erhalten.

Anstatt sich mit Root-Anmeldeinformationen bei Ihrem AWS Konto anzumelden oder Ihre Anmeldeinformationen mit anderen zu teilen, sollten Sie für sich selbst und für alle, die möglicherweise Zugriff auf ein Dokument oder eine Vereinbarung benötigen, eine spezielle Benutzeridentität, einen sogenannten IAM-Benutzer, einrichten. AWS Artifact Mit diesem Ansatz können Sie individuelle Anmeldedaten für jeden Benutzer bereitstellen. Sie können den einzelnen Benutzern nur die Berechtigungen erteilen, die sie für die Arbeit mit bestimmten Dokumenten benötigen. Sie können auch mehreren IAM-Benutzern dieselben Berechtigungen gewähren, indem Sie die Berechtigungen einer IAM-Gruppe gewähren und die IAM-Benutzer der Gruppe hinzufügen.

Wenn Sie Benutzeridentitäten bereits außerhalb verwaltenAWS, können Sie IAM-Identitätsanbieter verwenden, anstatt IAM-Benutzer zu erstellen. Weitere Informationen finden Sie unter Identitätsanbieter und Verbund im IAM-Benutzerhandbuch.

Inhalt

Benutzerzugriff einrichten für AWS Artifact

Gehen Sie wie folgt vor, um Benutzern AWS Artifact je nach benötigter Zugriffsebene Berechtigungen zu erteilen.

Aufgaben

Schritt 1: Erstellen einer IAM-Richtlinie

Als IAM-Administrator können Sie eine Richtlinie erstellen, die Berechtigungen für AWS Artifact Aktionen und Ressourcen gewährt.

So erstellen Sie eine IAM-Richtlinie

Gehen Sie wie folgt vor, um eine IAM-Richtlinie zu erstellen, mit der Sie Ihren IAM-Benutzern und -Gruppen Berechtigungen gewähren können.

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Policies aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie den Tab JSON.
5. Geben Sie ein Richtliniendokument ein. Sie können Ihre eigene Richtlinie erstellen oder eine der Richtlinien von verwendenIAM-Beispielrichtlinien.
6. Wählen Sie Review policy (Richtlinie überprüfen) aus. Die Richtlinienvalidierung meldet mögliche Syntaxfehler.
7. Geben Sie auf der Seite Richtlinie überprüfen einen eindeutigen Namen ein, anhand dessen Sie sich den Zweck der Richtlinie leichter merken können. Sie können auch eine Beschreibung angeben.
8. Wählen Sie Richtlinie erstellen aus.

Schritt 2: Erstellen Sie eine IAM-Gruppe und fügen Sie die Richtlinie an

Als IAM-Administrator können Sie eine Gruppe erstellen und die von Ihnen erstellte Richtlinie an die Gruppe anhängen. Sie können der Gruppe jederzeit IAM-Benutzer hinzufügen.

Um eine IAM-Gruppe zu erstellen und Ihre Richtlinie anzuhängen

1. Wählen Sie im Navigationsbereich Groups und Create New Group aus.

2. Geben Sie unter Gruppenname einen Namen für Ihre Gruppe ein und wählen Sie dann Next Step aus.
3. Geben Sie im Suchfeld den Namen der Richtlinie ein, die Sie erstellt haben. Aktivieren Sie das Kontrollkästchen für Ihre Richtlinie und wählen Sie dann Nächster Schritt aus.
4. Prüfen Sie den Gruppennamen und die Richtlinien. Wenn Sie bereit sind, wählen Sie Gruppe erstellen.

Schritt 3: Erstellen Sie IAM-Benutzer und fügen Sie sie der Gruppe hinzu

Als IAM-Administrator können Sie jederzeit Benutzer zu einer Gruppe hinzufügen. Dadurch werden den Benutzern die der Gruppe gewährten Berechtigungen gewährt.

Um einen IAM-Benutzer zu erstellen und den Benutzer einer Gruppe hinzuzufügen

1. Wählen Sie im Navigationsbereich Users (Benutzer) und dann Add User (Benutzer hinzufügen) aus.
2. Geben Sie unter Benutzername die Namen für einen oder mehrere Benutzer ein.
3. Aktivieren Sie das Kontrollkästchen neben AWS Management Console access (Konsolenzugriff). Konfigurieren Sie ein automatisch generiertes oder benutzerdefiniertes Passwort. Sie können optional „Benutzer muss bei der nächsten Anmeldung ein neues Passwort erstellen“ auswählen, damit das Passwort bei der ersten Anmeldung zurückgesetzt werden muss.
4. Wählen Sie Weiter: Berechtigungen aus.
5. Wählen Sie Benutzer zur Gruppe hinzufügen und wählen Sie dann die Gruppe aus, die Sie erstellt haben.
6. Wählen Sie Weiter: Markierungen. Sie können Ihren Benutzern optional Tags hinzufügen.
7. Wählen Sie Weiter: Prüfen aus. Wenn Sie bereit sind, wählen Sie Benutzer erstellen.

Migration zu fein abgestuften Berechtigungen

AWSArtifact ermöglicht es Kunden jetzt, detaillierte Berechtigungen zu verwenden. Durch diese detaillierten Berechtigungen haben Kunden eine detaillierte Kontrolle darüber, wie sie Zugriff auf Funktionen wie das Akzeptieren von Bedingungen und das Herunterladen von Berichten gewähren.

Um mithilfe der detaillierten Berechtigungen auf Berichte zuzugreifen, können Sie die AWSArtifactReportsReadOnlyAccessverwaltete Richtlinie verwenden oder Ihre Berechtigungen

gemäß der folgenden Empfehlung aktualisieren. Wenn Sie sich zuvor gegen die Verwendung detaillierter Berechtigungen entschieden haben, sollten Sie sich über den Link „Opt-In für detaillierte Berechtigungen für AWS Artifact-Berichte anmelden“ in der Berichtskonsole anmelden.

Sie haben die Möglichkeit, über den Link „Die detaillierten Berechtigungen für AWS Artifact-Berichte deaktivieren“ in der Konsole auf die Berichte mit alten Berechtigungen zuzugreifen, falls bei der Aktualisierung auf die neuen Berechtigungen ein Problem auftritt.

Migration zu neuen Berechtigungen

Migrieren Sie nicht ressourcenspezifische Berechtigungen

Benutzer müssen die bestehende Richtlinie mit älteren Berechtigungen durch eine Richtlinie mit detaillierten Berechtigungen ersetzen

Legacy-Richtlinie:

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

Neue Richtlinie mit detaillierten Berechtigungen:

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

```
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

Migrieren Sie ressourcenspezifische Berechtigungen

Benutzer müssen ihre bestehende Richtlinie mit veralteten Berechtigungen durch eine Richtlinie mit detaillierten Berechtigungen ersetzen. Platzhalterberechtigungen für Berichtsressourcen wurden durch Bedingungsschlüssel ersetzt.

Legacy-Richtlinie:

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

Neue Richtlinie mit detaillierten Berechtigungen und Bedingungsschlüsseln.

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

IAM-Beispielrichtlinien

Sie können Berechtigungsrichtlinien erstellen, die IAM-Benutzern Berechtigungen gewähren. Sie können Benutzern Zugriff auf AWS Artifact Berichte gewähren und ihnen die Möglichkeit geben, Vereinbarungen entweder im Namen eines einzelnen Kontos oder einer Organisation anzunehmen und herunterzuladen.

Die folgenden Beispielrichtlinien zeigen Berechtigungen, die Sie IAM-Benutzern auf der Grundlage der benötigten Zugriffsebene zuweisen können.

- Beispielrichtlinien für die Verwaltung von AWS Berichten mit detaillierten Berechtigungen
- Beispielrichtlinien für die Verwaltung von Berichten von Drittanbietern
- Beispielrichtlinien zur Verwaltung von Vereinbarungen

- Beispielrichtlinien zur Integration AWS Organizations
- Beispielrichtlinien zur Verwaltung von Vereinbarungen für das Verwaltungskonto
- Beispielrichtlinien für die Verwaltung von Organisationsvereinbarungen
- Beispielrichtlinien zur Verwaltung von Benachrichtigungen

Example Beispielrichtlinien für die Verwaltung von AWS Berichten mithilfe detaillierter Berechtigungen

> **Tip**
>
> Sie sollten erwägen, die AWSArtifactReportsReadOnlyAccess verwaltete Richtlinie zu verwenden, anstatt Ihre eigene Richtlinie zu definieren.

Die folgende Richtlinie gewährt die Erlaubnis, alle AWS Berichte mithilfe detaillierter Berechtigungen herunterzuladen.

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

Die folgende Richtlinie gewährt die Erlaubnis, nur die AWS SOC-, PCI- und ISO-Berichte herunterzuladen, und zwar mithilfe detaillierter Berechtigungen.

```
{
  "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 Beispielrichtlinien für die Verwaltung von Berichten von Drittanbietern

> **Tip**
>
> Sie sollten erwägen, die AWSArtifactReportsReadOnlyAccess verwaltete Richtlinie zu verwenden, anstatt Ihre eigene Richtlinie zu definieren.

Berichte von Drittanbietern werden mit der IAM-Ressource gekennzeichnet. `report`

Die folgende Richtlinie gewährt Zugriff auf alle Berichtsfunktionen von Drittanbietern.

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

```
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

Die folgende Richtlinie gewährt die Genehmigung zum Herunterladen von Berichten von Drittanbietern.

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

Die folgende Richtlinie gewährt die Erlaubnis, Berichte von Drittanbietern aufzulisten.

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

Die folgende Richtlinie gewährt die Erlaubnis, die Details eines Drittanbieterberichts für alle Versionen einzusehen.

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

Die folgende Richtlinie gewährt die Erlaubnis, die Details eines Drittanbieter-Berichts für eine bestimmte Version einzusehen.

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

Example Beispielrichtlinien zur Verwaltung von Vereinbarungen

Die folgende Richtlinie gewährt die Erlaubnis, alle Vereinbarungen herunterzuladen. IAM-Benutzer müssen ebenfalls über diese Berechtigung verfügen, um Vereinbarungen akzeptieren zu können.

```
{
```

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

Die folgende Richtlinie gewährt die Erlaubnis, eine Vereinbarung anzunehmen.

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

Die folgende Richtlinie gewährt die Erlaubnis, eine Vereinbarung zu kündigen.

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

```
        "*"
      ]
    }
  ]
}
```

Die folgende Richtlinie gewährt Berechtigungen zur Verwaltung von Einzelkontenvereinbarungen.

```
{
  "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 Beispielrichtlinien für die Integration AWS Organizations

Die folgende Richtlinie erteilt die Erlaubnis, die IAM-Rolle zu erstellen, die für die Integration mit AWS Artifact AWS Organizations verwendet wird. Das Verwaltungskonto Ihrer Organisation muss über diese Berechtigungen verfügen, um mit Organisationsvereinbarungen beginnen zu können.

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

Die folgende Richtlinie erteilt die Erlaubnis, AWS Artifact die Nutzungsberechtigungen zu erteilen AWS Organizations. Das Verwaltungskonto Ihrer Organisation muss über diese Berechtigungen verfügen, um mit Organisationsvereinbarungen beginnen zu können.

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

Example Beispielrichtlinien zur Verwaltung von Vereinbarungen für das Verwaltungskonto

Die folgende Richtlinie gewährt Berechtigungen zur Verwaltung von Vereinbarungen für das Verwaltungskonto.

```
{
  "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 Beispielrichtlinien für die Verwaltung von Organisationsvereinbarungen

Die folgende Richtlinie gewährt Berechtigungen zur Verwaltung von Organisationsvereinbarungen. Ein anderer Benutzer mit den erforderlichen Berechtigungen muss die Organisationsvereinbarungen einrichten.

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

Die folgende Richtlinie gewährt Berechtigungen zum Einsehen von Organisationsvereinbarungen.

```
{
  "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 Beispielrichtlinien zur Verwaltung von Benachrichtigungen

Die folgende Richtlinie gewährt vollständige Berechtigungen zur Verwendung von AWS Artifact Benachrichtigungen.

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

Die folgende Richtlinie gewährt die Erlaubnis, alle Konfigurationen aufzulisten.

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

Die folgende Richtlinie erteilt die Erlaubnis, eine Konfiguration zu erstellen.

```
{
  "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": [
```

```
        "*"
      ]
    }
  ]
}
```

Die folgende Richtlinie gewährt die Erlaubnis, eine Konfiguration zu bearbeiten.

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

Die folgende Richtlinie gewährt die Erlaubnis, eine Konfiguration zu löschen.

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

```
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Die folgende Richtlinie gewährt die Erlaubnis, Details einer Konfiguration anzuzeigen.

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

Die folgende Richtlinie erteilt die Erlaubnis, Notification Hubs zu registrieren oder deren Registrierung aufzuheben.

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

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

AWSverwaltete Richtlinien für AWS Artifact

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWSverwaltete Richtlinie: AWSArtifactReportsReadOnlyAccess

Sie können die `AWSArtifactReportsReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt *nur Leseberechtigungen*, die das Auflisten, Anzeigen und Herunterladen von Berichten ermöglichen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `artifact`— Ermöglicht Prinzipalen das Auflisten, Anzeigen und Herunterladen von Berichten von. AWS Artifact

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

Artefakt-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Artifact an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Seite mit dem Verlauf von Artifact Document, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
Artifact hat begonnen, Änderungen zu verfolgen	Artifact begann mit der Nachverfolgung von	2023-12-15

Änderung	Beschreibung	Datum
	Änderungen für seine AWS verwalteten Richtlinien und führte ein AWSArtifactReports ReadOnlyAccess.	

Verwenden von serviceverknüpften Rollen für AWS Artifact

AWS Artifact verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit AWS Artifact verknüpft ist. Servicebezogene Rollen sind von AWS Artifact vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von AWS Artifact, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Artifact definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur AWS Artifact seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen juristischen Stelle von IAM zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre AWS Artifact-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entziehen können.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Servicebezogene Rollenberechtigungen für AWS Artifact

AWS Artifact verwendet die servicebezogene Rolle mit dem Namen AWSServiceRoleForArtifact—Ermöglicht AWS Artifact, Informationen über eine Organisation über den Service AWS Organizations zu sammeln.

Die AWSServiceRoleForArtifact serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle übernehmen:

- `artifact.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSArtifactServiceRolePolicy ermöglicht es AWS Artifact, die folgenden Aktionen auf der `organizations` Ressource durchzuführen.

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

Eine serviceverknüpfte Rolle für AWS Artifact erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die Registerkarte Organisationsvereinbarungen in einem Organisationsverwaltungskonto aufrufen und dort den Link „Erste Schritte“ auswählenAWS Management Console, erstellt AWS Artifact die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie die Registerkarte Organisationsvereinbarungen in einem Organisationsverwaltungskonto aufrufen und den Link „Erste Schritte“ auswählen, erstellt AWS Artifact die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für AWS Artifact

Mit AWS Artifact können Sie die AWSServiceRoleForArtifact serviceverknüpfte Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Artifact

Wenn Sie eine Funktion oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der AWS Artifact-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AWS Artifact-Ressourcen zu löschen, die verwendet werden von AWSServiceRoleForArtifact

1. Besuchen Sie die Tabelle „Organisationsvereinbarungen“ in der AWS Artifact-Konsole
2. Kündigen Sie alle aktiven Organisationsvereinbarungen

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS APIAWS CLI, um die AWSServiceRoleForArtifact serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für Rollen im Zusammenhang mit dem Service von AWS Artifact

AWS Artifact unterstützt nicht die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Sie können die AWSServiceRoleForArtifact Rolle in den folgenden Regionen verwenden.

Name der Region	Regions-ID	Support in AWS Artifact
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Nein
USA West (Nordkalifornien)	us-west-1	Nein
USA West (Oregon)	us-west-2	Ja
Afrika (Kapstadt)	af-south-1	Nein
Asien-Pazifik (Hongkong)	ap-east-1	Nein

Name der Region	Regions-ID	Support in AWS Artifact
Asien-Pazifik (Jakarta)	ap-southeast-3	Nein
Asien-Pazifik (Mumbai)	ap-south-1	Nein
Asien-Pazifik (Osaka)	ap-northeast-3	Nein
Asien-Pazifik (Seoul)	ap-northeast-2	Nein
Asien-Pazifik (Singapur)	ap-southeast-1	Nein
Asien-Pazifik (Sydney)	ap-southeast-2	Nein
Asien-Pazifik (Tokio)	ap-northeast-1	Nein
Kanada (Zentral)	ca-central-1	Nein
Europa (Frankfurt)	eu-central-1	Nein
Europa (Irland)	eu-west-1	Nein
Europa (London)	eu-west-2	Nein
Europa (Mailand)	eu-south-1	Nein
Europa (Paris)	eu-west-3	Nein
Europa (Stockholm)	eu-north-1	Nein
Naher Osten (Bahrain)	me-south-1	Nein
Naher Osten (VAE)	me-central-1	Nein
South America (São Paulo)	sa-east-1	Nein
AWS GovCloud (US-Ost)	us-gov-east-1	Nein
AWS GovCloud (US-West)	us-gov-west-1	Nein

Verwenden von IAM-Bedingungsschlüsseln

Sie können IAM-Bedingungsschlüssel verwenden, um einen differenzierten Zugriff auf Berichte auf AWS Artifact zu ermöglichen, die auf bestimmten Berichtskategorien und -serien basieren.

Die folgenden Beispielrichtlinien zeigen Berechtigungen, die Sie IAM-Benutzern auf der Grundlage bestimmter Berichtskategorien und -serien zuweisen können.

Example Beispielrichtlinien zur Verwaltung des Lesezugriffs auf AWS Berichte

AWS ArtifactBerichte werden durch die IAM-Ressource gekennzeichnet,. `report`

Die folgende Richtlinie gewährt die Erlaubnis, alle AWS Artifact Berichte dieser Kategorie zu lesen. `Certifications and Attestations`

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

Mit der folgenden Richtlinie können Sie die Erlaubnis erteilen, alle AWS Artifact Berichte der SOC Serie zu lesen.

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

Mit der folgenden Richtlinie können Sie die Leseberechtigung für alle AWS Artifact Berichte mit Ausnahme der Berichte dieser `Certifications and Attestations` Kategorie erteilen.

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

Protokollierung von AWS Artifact-API-Aufrufen mit AWS CloudTrail

AWS Artifactist in einen Dienst integriertAWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurdenAWS Artifact. CloudTrail erfasst API-Aufrufe AWS Artifact als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Artifact-Konsole und Code-Aufrufe der AWS Artifact-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen fürAWS Artifact. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurdeAWS Artifact, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Informationen.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrailBenutzerhandbuch.

AWS ArtifactInformationen in CloudTrail

CloudTrail ist auf Ihrem aktiviertAWS-Konto, wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindetAWS Artifact, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Artifact, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails

- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

AWS Artifactunterstützt die Protokollierung der folgenden Aktionen als Ereignisse in CloudTrail Protokolldateien:

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu AWS Artifact-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die GetReportMetadata Aktion demonstriert.


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

Dokumentverlauf für AWS Artifact

In der folgenden Tabelle werden die Veröffentlichungen für AWS Artifact beschrieben.

Änderung	Beschreibung	Datum
Detaillierter Berichtszugriff und verwaltete Richtlinien AWSArtifactReportReadOnlyAccess	Der detaillierte Zugriff auf Artifact Reports wurde aktiviert, die Bedingungsschlüssel für Berichte aktiviert und die verwaltete Richtlinie gestartetAWSArtifactReportsReadOnlyAccess .	15. Dezember 2023
Mit dem Service verknüpfte Rolle mit AWS Artifact	Servicebezogene Rollendokumentation und aktualisierte Beispielrichtlinien für die Integration von AWS Artifact und AWS Organizations hinzugefügt.	26. September 2023
Benachrichtigungen	Die Dokumentation zur Verwaltung von Benachrichtigungen wurde veröffentlicht und relevante Aktualisierungen am API-Referenzhandbuch, der CloudTrail Protokollierungsdokumentation und der Seite AWS Artifact Identity and Access Management vorgenommen.	1. August 2023
Berichte von Drittanbietern — Allgemein verfügbar	API-Referenzdokumentation und CloudTrail Protokollierungsdokumentation wurden hinzugefügt und Berichte	27. Januar 2023

	von Drittanbietern allgemein verfügbar gemacht.	
Berichte von Drittanbietern (Vorschau)	Veröffentlichung von Compliance-Berichten der unabhängigen Softwarea nbieter (ISVs), an die sie ihre Produkte verkaufen. AWS Marketplace Außerdem wurden der Seite „Identitä ts- und Zugriffsverwaltung“ Beispielrichtlinien für Berichte von Drittanbietern hinzugefügt.	30. November 2022
Sicherheit	Der Seite zur Identitäts- und Zugriffsverwaltung wurde ein Abschnitt hinzugefügt, in dem Sie verhindern können, dass Ihr Stellvertreter verwirrt ist.	20. Dezember 2021
Berichte	Die Geheimhaltungsvere inbarung wurde entfernt und die Nutzungsbedingungen für das Herunterladen von Berichten wurden eingeführt.	17. Dezember 2020
Startseite und Suche	Service-Homepage und Suchleiste auf der Seite „Berichte und Vereinbarungen“ hinzugefügt.	15. Mai 2020
GovCloud starten	AWS ArtifactIn GovCloud Regionen eingeführt.	7. November 2019
AWS OrganizationsVerei nbarungen	Unterstützung für die Verwaltung von Vereinbar ungen für eine Organisation hinzugefügt.	20. Juni 2018

Vereinbarungen	Unterstützung für die Verwaltung von AWS Artifact Vereinbarungen hinzugefügt.	17. Juni 2017
Erstversion	Mit dieser Version wird AWS Artifact eingeführt.	30. November 2016

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.