ユーザーガイド

AWS Artifact

AWS Artifact: ユーザーガイド

Table of Contents

とは AWS Artifact

AWS Artifact は、 AWS セキュリティおよびコンプライアンスドキュメントのオンデマンドダウンロードを提供します。例えば、国際標準化機構 (ISO) 標準および Payment Card Industry (PCI) セキュリティ標準、および System and Organization Controls (SOC) レポートへの準拠に関するレポートです。 は、 AWS セキュリティコントロールの実装と運用の有効性を検証する認定機関からの証明書のダウンロード AWS Artifact も提供します。

では AWS Artifact、 で製品を販売する独立系ソフトウェアベンダー (ISVs) のセキュリティおよびコンプライアンスに関するドキュメントをダウンロードすることもできます AWS Marketplace。詳細については、「AWS Marketplace ベンダーインサイト」を参照してください。

さらに、 AWS Artifact を使用して、組織 AWS アカウント 内の AWS および の複数の との契約のステータスを確認、承認 AWS アカウント 、追跡できます。のアグリーメントの詳細については AWS Artifact、「」を参照してくださいでの契約の管理 AWS Artifact。

使用する AWS インフラストラクチャとサービスのセキュリティとコンプライアンスを実証するために、監査アーティファクトとして監査者または規制当局に AWS Artifact ドキュメントを送信できます。これらの監査アーティファクトをガイドラインとして使用して、独自のクラウドアーキテクチャを評価し、会社の内部統制の有効性を評価することもできます。監査アーティファクトの詳細については、AWS Artifact FAQs「」を参照してください。

> **Note**
>
> AWS お客様は、会社のセキュリティとコンプライアンスを証明するドキュメントを作成または取得する責任があります。詳細については、「責任共有モデル」を参照してください。

料金

AWS は、 AWS Artifact ドキュメントと契約を無料で提供します。

の開始方法 AWS Artifact

の使用を開始するには AWS Artifact、 AWS Artifact コンソールでその主要な機能を試します。コンソールでは、 AWS セキュリティおよびコンプライアンスレポートをダウンロードし、法的契約をダウンロードして承諾し、 AWS Artifact ドキュメントに関する通知をサブスクライブできます。

前提条件

の機能を使用するには AWS Artifact、 が必要です AWS アカウント。セットアップ手順については、「 セットアップユーザーガイド」の「新しい AWS アカウント AWS をセットアップする」を参照してください。

機能

の機能の使用方法については AWS Artifact、次のトピックを参照してください。

- レポートをダウンロードする
- 契約の管理
- 通知の設定

でのレポートのダウンロード AWS Artifact

AWS Artifact コンソールからレポートをダウンロードすることができます。からレポートをダウンロードすると AWS Artifact、レポートはお客様専用に生成され、すべてのレポートに一意の透かしがあります。このため、レポートは信頼しているユーザーとのみ共有してください。添付ファイルとしてレポートを E メールで送信したり、オンラインで共有したりしないでください。レポートを共有するには、Amazon などの安全な共有サービスを使用します WorkDocs。一部のレポートでは、ダウンロードする前に規約に同意する必要があります。

内容

レポートをダウンロードする

レポートをダウンロードするには、必須のアクセス許可が必要です。詳細については、「での Identity and Access Management AWS Artifact」を参照してください。

にサインアップすると AWS Artifact、アカウントには一部のレポートをダウンロードするアクセス許可が自動的に付与されます。へのアクセスに問題がある場合は AWS Artifact、AWS Artifact サービス認可リファレンスページのガイダンスに従ってください。

レポートをダウンロードするには

1. で AWS Artifact コンソールを開きますhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ホームページで、レポートの表示 を選択します。

   レポートページのAWS レポートタブで、 AWS レポートにアクセスできます (SOC1/2/3、PCI、C5 など) 。サードパーティーレポートタブでは、 で製品を販売する独立系ソフトウェアベンダー (ISVs) からのレポートにアクセスできます AWS Marketplace。
3. (オプション) レポートを検索するには、検索フィールドにキーワードを入力します。レポートのタイトル、カテゴリ、シリーズ、説明など、個々の列に基づいてレポートのターゲット検索を実行することもできます。例えば、Cloud Computing Compliance Controls Catalogue (C5) レ

ポートを検索するには、「Title」、「contains」演算子 (:)、「C5」という用語 () を使用してタイトル列を検索できます**`Title : C5`**。

4. (オプション) レポートの詳細については、レポートのタイトルを選択して詳細ページを開きます。
5. レポートを選択し、[レポートのダウンロード] を選択します。
6. ダウンロードする特定のレポートの利用規約 (レポートをダウンロードする条件を受け入れる) に同意するように求められる場合があります。利用規約をよくお読みになることをお勧めします。読み終わったら、「I have read and agree to the terms」を選択し、「Accept terms and download report」を選択します。
7. ダウンロードしたファイルをビューPDFワーで開きます。同意に関する規約を確認し、下にスクロールして監査レポートを探してください。レポートにはPDF、ドキュメント内の添付ファイルとして追加情報が埋め込まれている可能性があるため、PDFファイル内の添付ファイルをチェックして、裏付けとなるドキュメントを確認してください。添付ファイルを表示する方法については、「」を参照してくださいPDF ドキュメントでの添付ファイルの表示。

PDF ドキュメントでの添付ファイルの表示

現在PDF添付ファイルの表示をサポートしている以下のアプリケーションをお勧めします。

Adobe Acrobat Reader

Adobe ウェブサイトの から最新バージョンの Adobe Acrobat Reader をダウンロードしますhttps://get.adobe.com/reader/。

Acrobat Reader でPDFアタッチメントを表示する方法については、Adobe Support ウェブサイトの「リンクとアタッチメントPDFs」を参照してください。

Firefox ブラウザ

1. Mozilla ウェブサイト https://www.mozilla.org/en-US/firefox/new/ から最新の Firefox ウェブブラウザをダウンロードします。
2. Firefox の組み込みPDFビューワーで PDF ファイルを開きます。手順については、「Firefox でPDFファイルを表示する」または「Mozilla サポート」ウェブサイトで別のビューワーを選択します。
3. Firefox の組み込みPDFビューワーでPDF添付ファイルを表示するには、サイドバー の切り替え、添付ファイルの表示 を選択します。

ドキュメントのセキュリティで保護する

AWS Artifact ドキュメントは機密であり、常に安全に保つ必要があります。 は、ドキュメントに責任 AWS 共有モデル AWS Artifact を使用します。つまり、 AWS は、 AWS クラウドにいる間、ドキュメントのセキュリティを維持する責任がありますが、ダウンロード後にドキュメントのセキュリティを維持する責任があります。ドキュメントをダウンロードする前に、利用規約に同意する必要がある AWS Artifact 場合があります。各ドキュメントのダウンロードには一意のトレース可能なウォーターマークが含まれます。

機密とマークされているドキュメントは、企業内、規制機関、およびお客様の監査人とのみ共有できます。これらのドキュメントをお客様の顧客またはウェブサイト上で共有することは許可されていません。Amazon などの安全なドキュメント共有サービスを使用して WorkDocs、他のユーザーとドキュメントを共有することを強くお勧めします。ドキュメントは E メール経由で送信したり、セキュアでないサイトにアップロードしたりしないでください。

トラブルシューティング

ドキュメントをダウンロードできない場合やエラーメッセージが表示された場合は、「」の「トラブルシューティング」を参照してください AWS Artifact FAQ。

での契約の管理 AWS Artifact

AWS Artifact を使用して、 AWS アカウント または組織の契約を確認および管理できます。例えば、医療保険の相互運用性と説明責任に関する法律 (HIPAA) の対象となる企業では、保護対象の医療情報 (BAA) が適切に保護されるように AWS するために、通常、事業提携契約 (PHI) を と締結する必要があります。 AWS Artifact コンソールでは、このような契約を確認して受諾し、法的 AWS アカウント に を処理できる を指定できますPHI。

を使用する場合は AWS Organizations、組織 AWS アカウント 内のすべての に代わって AWS、BAAとの などの契約を受諾できます。既存のメンバーアカウントとそれ以降のすべてのメンバーアカウントは、自動的に契約の対象となり、法的に を処理できますPHI。

AWS Artifact を使用して、お客様 AWS アカウント または組織が契約を受諾したことを確認し、受諾された契約の条項を確認してお客様の義務を理解することもできます。アカウントまたは組織が受諾済みの契約を使用する必要がなくなった場合は、 AWS Artifact を使用して契約を終了できます。契約を終了しても、後でその契約が必要であることに気付いた場合は、契約を再度アクティブ化できます。

内容

AWS アカウント での の契約への同意 AWS Artifact

AWS Artifact コンソールを使用して、 AWS の との契約を確認して受諾できます AWS アカウント。

> **Important**
>
> 契約を受諾する前に、法務、個人情報、およびコンプライアンス担当部門に相談することをお勧めします。

必要なアクセス許可

アカウントの管理者は、1 つ以上の契約にアクセスして管理するアクセス許可をIAMユーザーとフェデレーティッドユーザーに付与できます。デフォルトでは、管理者権限を持つユーザーしか契約を受諾できません。契約を受諾するには、 IAMおよびフェデレーティッドユーザーに必要なアクセス許可が必要です。

詳細については、「での Identity and Access Management AWS Artifact」を参照してください。

との契約を受諾するには AWS

1. で AWS Artifact コンソールを開きますhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ナビゲーションペインで、契約を選択します。
3. [アカウント契約] タブを選択します。
4. で AWS Artifact コンソールを開きますhttps://console.aws.amazon.com/artifact/。
5. ナビゲーションペインで、契約を選択します。
6. 契約ページで、次のいずれかを実行します。
   - 自分のアカウントでのみ契約を受諾するには、アカウント契約タブを選択します。
   - 組織に代わって契約を受諾するには、組織契約タブを選択します。
7. 契約を選択し、契約のダウンロードを選択します。

   ダウンロードNDAを受け入れるダイアログボックスが表示されます。
8. 選択した契約をダウンロードする前に、まず機密保持契約 () AWS Artifact の条項に同意する必要がありますAWS Artifact NDA。

   a. レポートのダウンロードNDAを承諾ダイアログボックスで、 を確認します AWS Artifact NDA。

   b. （ オプション) のコピーを印刷するには AWS Artifact NDA (または として保存するには PDF ）、印刷 NDAを選択します。

   c. 「」を選択し、「」のすべての条項を読み、同意しますNDA。

   d. を AWS Artifact NDA承諾し、選択したPDF契約の をダウンロードするには、承諾NDAしてダウンロードを選択します。
9. PDF ビューワーで、ダウンロードPDFした契約を確認します。
10. AWS Artifact コンソールで、契約を選択した状態で、契約に同意を選択します。
11. 「同意」ダイアログボックスで、次の操作を行います。

    a. 契約を確認します。

b. 選択 これらのすべての利用規約に同意します。

c. 契約に同意を選択します。

12. [Accept] (同意する) を選択して自分のアカウントの契約を受諾します。

AWS アカウント での の契約の終了 AWS Artifact

AWS Artifact コンソールを使用して単一の の契約を受諾 AWS アカウントした場合は、コンソールを使用してその契約を終了できます。それ以外の場合は、「でのオフライン契約 AWS Artifact」を参照してください。

必要なアクセス許可

契約を終了するには、 IAMおよびフェデレーティッドユーザーが必要なアクセス許可を持っている必要があります。

詳細については、「での Identity and Access Management AWS Artifact」を参照してください。

とのオンライン契約を終了するには AWS

1. で AWS Artifact コンソールを開きますhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ナビゲーションペインで、契約を選択します。
3. [アカウント契約] タブを選択します。
4. 契約を選択し、[Terminate agreement] (契約を終了) を選択します。
5. すべてのチェックボックスをオンにして、契約の終了に同意することを示します。
6. [Terminate] (終了) を選択します。確認を求めるメッセージが表示されたら、[終了] を選択します。

での組織との契約の受諾 AWS Artifact

AWS Organizations 組織の管理アカウントの所有者は、組織 AWS アカウント 内のすべての AWS に代わって との契約を受諾できます。

> **Important**
>
> 契約を受諾する前に、法務、個人情報、およびコンプライアンス担当部門に相談することをお勧めします。

AWS Organizations には、一括請求機能とすべての機能の 2 つの機能セットがあります。組織 AWS Artifact で を使用するには、所属する組織をすべての機能で有効にする必要があります。組織が一括請求用にのみ設定されている場合は、AWS Organizations ユーザーガイドの「組織内のすべての機能の有効化」を参照してください。

組織契約を受諾または終了するには、適切な AWS Artifact アクセス許可で管理アカウントにサインインする必要があります。アクセス`organizations:DescribeOrganization`許可を持つメンバーアカウントのユーザーは、ユーザーに代わって承諾された組織契約を表示できます。

詳細については、「 AWS Organizations ユーザーガイド」の「 を使用した組織内のアカウントの管理 AWS Organizations」を参照してください。

必要なアクセス許可

契約を受諾するには、管理アカウントの所有者に必要なアクセス許可が必要です。

詳細については、「での Identity and Access Management AWS Artifact」を参照してください。

組織の契約を受諾するには

1. で AWS Artifact コンソールを開きますhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ダッシュボードで、契約を選択します。
3. [Organization agreements (組織契約)] タブを選択します。
4. で AWS Artifact コンソールを開きますhttps://console.aws.amazon.com/artifact/。
5. ナビゲーションペインで、契約を選択します。
6. 契約ページで、次のいずれかを実行します。
   - アカウントのみの契約を受諾するには、アカウント契約タブを選択します。
   - 組織に代わって契約を受諾するには、組織契約タブを選択します。
7. 契約を選択し、契約のダウンロードを選択します。

   ダウンロードNDAを受け入れるダイアログボックスが表示されます。
8. 選択した契約をダウンロードする前に、まず機密保持契約 () AWS Artifact の条項に同意する必要がありますAWS Artifact NDA。

   a. レポートのダウンロードNDAを受け入れるダイアログボックスで、 を確認します AWS Artifact NDA。
   b. （ オプション) のコピーを印刷するには AWS Artifact NDA (または として保存するには PDF ）、印刷 NDAを選択します。

c. 「」を選択し、「」のすべての条項を読み、同意しますNDA。

d. を AWS Artifact NDA承諾し、選択したPDF契約の をダウンロードするには、承諾NDAしてダウンロードを選択します。

9. PDF ビューワーで、ダウンロードPDFした契約を確認します。

10. AWS Artifact コンソールで、契約を選択した状態で、契約に同意を選択します。

11. 「同意」ダイアログボックスで、次の操作を行います。

a. 契約を確認します。

b. 選択 これらのすべての利用規約に同意します。

c. 契約に同意を選択します。

12. Accept を選択して、組織内のすべての既存アカウントと将来のアカウントの契約を受諾します。

での組織の契約の終了 AWS Artifact

の組織内のすべてのメンバーアカウントに代わって AWS Artifact コンソールを使用して契約を受諾した場合は、 コンソールを使用してその契約を終了できます。 AWS Organizationsそれ以外の場合は、「でのオフライン契約 AWS Artifact」を参照してください。

メンバーアカウントが組織から削除された場合、そのメンバーアカウントは組織契約の対象範囲が長くなります。組織からメンバーアカウントを削除する前に、管理アカウントの管理者は、必要に応じて新しい契約を締結できるように、これをメンバーアカウントに伝える必要があります。アクティブな組織契約のリストは、 AWS Artifact コンソールの「契約」ページの「組織契約」で確認できます。

詳細については AWS Organizations、「 AWS Organizations ユーザーガイド」の「 を使用した組織内のアカウントの管理 AWS Organizations」を参照してください。

必要なアクセス許可

契約を終了するには、管理アカウントの所有者に必要なアクセス許可が必要です。

詳細については、「での Identity and Access Management AWS Artifact」を参照してください。

とのオンライン組織契約を終了するには AWS

1. で AWS Artifact コンソールを開きますhttps://console.aws.amazon.com/artifact/。

2. AWS Artifact ダッシュボードで、契約を選択します。
3. [Organization agreements (組織契約)] タブを選択します。
4. 契約を選択し、[Terminate agreement] (契約を終了) を選択します。
5. すべてのチェックボックスをオンにして、契約の終了に同意することを示します。
6. [Terminate] (終了) を選択します。確認を求めるメッセージが表示されたら、[終了] を選択します。

でのオフライン契約 AWS Artifact

既存のオフライン契約がある場合は、オフラインで承諾した契約が AWS Artifact に表示されます。例えば、コンソールにオフラインの事業提携契約 (BAA) がアクティブステータスで表示される場合があります。有効というステータスは契約が受諾されたことを示します。オフライン契約を終了するには、契約に含まれる終了のガイドラインおよび手順を参照してください。

アカウントが AWS Organizations 組織の管理アカウントである場合は、 AWS Artifact を使用して、オフライン契約の条項を組織内のすべてのアカウントに適用できます。オフラインで承諾した契約を組織および組織内のすべてのアカウントに適用するには、必要なアクセス許可が必要です。

アカウントが組織のメンバーアカウントである場合は、オフラインの組織契約を表示するためのアクセス許可が必要です。

詳細については、「での Identity and Access Management AWS Artifact」を参照してください。

での E メール通知の設定 AWS Artifact

AWS Artifact コンソールを使用して、 のアグリーメントとレポートの更新に関する E メール通知を設定できます AWS Artifact。 は、 を使用してこれらの E メール通知 AWS Artifact を送信します AWS User Notifications。E メール通知を受信する AWS Artifact には、まず User Notifications コンソールで AWS User Notifications 通知ハブを選択する必要があります。次に、 AWS Artifact コンソールで、通知の受信者と受信する通知を指定する通知設定を作成できます。

E AWS Artifact メール通知を設定するには、 AWS Artifact と に必要なアクセス許可が必要です AWS User Notifications。詳細については、「での Identity and Access Management AWS Artifact」を参照してください。

内容

前提条件: で通知ハブを選択する User Notifications

E AWS Artifact メール通知を受信する前に、まず User Notifications コンソールを開き、データを保存する AWS リージョン User Notifications で通知ハブを選択する必要があります。通知ハブの選択は AWS User Notifications、 AWS Artifact が通知の送信に使用する に必要です。

通知ハブを選択するには

1. AWS User Notifications コンソールの通知ハブページを開きます。
2. AWS User Notifications リソース AWS リージョン を保存する の通知ハブを選択します。デフォルトでは、 User Notifications データは米国東部 (バージニア北部) リージョンに保存されます。 は、選択した他のリージョンに通知データを User Notifications レプリケートします。詳細については、AWS User Notifications 「 ユーザーガイド」の通知ハブのドキュメントを参照してください。
3. [Save and continue] を選択します。

AWS Artifact 通知設定の設定の作成

User Notifications 通知ハブ を選択したら、 AWS Artifact コンソールで通知設定の設定を作成できます。作成する設定で、 AWS Artifact 通知を受信する受信者の E メールアドレスを指定します。また、 AWS Artifact アグリーメントの更新や、すべての (またはサブセットの) AWS Artifact レポートの更新など、受信者が通知を受け取る更新も指定します。

設定を作成するには

1. AWS Artifact コンソールの通知設定ページを開きます。
2. [Create configuration] (設定を作成) をクリックします。
3. 設定の作成ページで、次の操作を行います。
    - アグリーメントの通知を受け取るには、アグリーメント で、 AWS アグリーメントの更新が選択されたままになります。
    - レポートの通知を受信するには、 レポート で、 AWS レポートの更新を選択したままにします。

        a. すべてのレポートの通知を受け取るには、すべてのレポート を選択します。

        b. 特定のカテゴリとシリーズに属するレポートについてのみ通知を受け取るには、レポートのサブセット を選択します。次に、関心のあるカテゴリとシリーズを選択します。
    - 設定名 に、設定の名前を入力します。
    - E メール の受信者 に、 AWS Artifact 通知 E メールを受信する E メールアドレスのカンマ区切りリストを入力します。
    - (オプション) 通知設定にタグを追加するには、タグ を展開し、新しいタグ を追加 を選択し、キーと値のペアとしてタグを入力します。 User Notifications リソースのタグ付けの詳細については、AWS User Notifications 「 ユーザーガイド」のAWS User Notifications 「リソースのタグ付け」を参照してください。
    - [Create configuration] (設定を作成) をクリックします。

        User Notifications は、指定した各受信者の E メールアドレスに検証 E メールを送信します。E メールアドレスを確認するには、検証 E メールの受信者が E メールの確認 を選択する必要があります。検証済みの E メールアドレスのみが AWS Artifact 通知を受け取ります。

AWS Artifact 通知設定の設定の編集

AWS Artifact 通知設定の設定を作成したら、いつでも設定を編集して通知設定を変更できます。例えば、受信者を追加または削除するには、受信する通知のタイプを変更し、タグを追加または削除します。

設定を編集するには

1. AWS Artifact コンソールの通知設定ページを開きます。
2. 編集する設定を選択します。
3. [編集] を選択します。
4. 設定の選択とフィールドを編集します。完了したら、変更の保存 を選択します。

   通知受信者として新しい E メールアドレスを追加した場合、 AWS User Notifications はそれらの E メールアドレスを検証 E メールを送信します。E メールアドレスを確認するには、検証 E メールの受信者が E メールの確認 を選択する必要があります。検証済みの E メールアドレスのみが AWS Artifact 通知を受け取ります。

AWS Artifact 通知設定の設定の削除

AWS Artifact 通知設定用に作成した設定が不要になった場合は、 AWS Artifact コンソールで設定を削除できます。

設定を削除するには

1. AWS Artifact コンソールの通知設定ページを開きます。
2. 削除する設定を選択します。
3. [削除] を選択します。
4. 設定の削除ダイアログボックスで、「削除」を選択します。

での Identity and Access Management AWS Artifact

にサインアップするときは AWS、 AWS アカウントに関連付けられた E メールアドレスとパスワードを指定します。これらはルート認証情報であり、 AWS リソースを含むすべての リソースへの完全なアクセスを提供します AWS Artifact。ただし、日常のアクセスにはルートアカウントを使用しないことを強くお勧めします。また、他のユーザーとアカウント認証情報を共有して、アカウントへの完全なアクセスを提供しないことをお勧めします。

ルート認証情報を使用して AWS アカウントにサインインしたり、他のユーザーと認証情報を共有したりするのではなく、自分自身と、 のドキュメントや契約にアクセスする必要がある可能性のあるユーザーのために、 ユーザーと呼ばれる特別なIAMユーザー ID を作成する必要があります AWS Artifact。この方法では、各ユーザーに個別のサインイン情報を提供し、各ユーザーが特定のドキュメントを使うために必要なアクセス許可のみを与えることができます。複数の IAM ユーザーに同じアクセス許可を付与するには、IAM グループにアクセス許可を付与して、IAM ユーザーをそのグループに追加します。

外部でユーザー ID をすでに管理している場合は AWS、IAMユーザーを作成する代わりに IAM ID プロバイダーを使用できます。詳細については、「 IAMユーザーガイド」の「ID プロバイダーとフェデレーション」を参照してください。

内容

- へのユーザーアクセスの許可 AWS Artifact
- のきめ細かなアクセス許可へのレポートの移行 AWS Artifact
- AWS アーティファクト契約のきめ細かなアクセス許可への移行
- のIAMポリシーの例 AWS Artifact
- の AWS 管理ポリシーの使用 AWS Artifact
- AWS Artifactのサービスにリンクされたロールの使用
- AWS Artifact レポートのIAM条件キーの使用

へのユーザーアクセスの許可 AWS Artifact

必要なアクセスレベル AWS Artifact に基づいて へのアクセス許可をユーザーに付与するには、次のステップを実行します。

タスク

ステップ 1: IAM ポリシーを作成する

IAM 管理者は、 AWS Artifact アクションとリソースへのアクセス許可を付与するポリシーを作成できます。

IAM ポリシーを作成するには

次の手順を使用して、IAMユーザーとグループに許可を付与するために使用できるIAMポリシーを作成します。

1. でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、ポリシー を選択します。
3. [ポリシーの作成] を選択します。
4. JSON タブを選択します。
5. ポリシードキュメントを入力します。独自のポリシーを作成するか、のIAMポリシーの例 AWS Artifact のポリシーを使用することもできます。
6. [ポリシーの確認] を選択します。構文エラーがある場合は、ポリシーバリデータが報告します。
7. [ポリシーの確認] ページで、ポリシーの目的を示す一意の名前を入力します。説明を追加することもできます。
8. [Create policy] を選択します。

ステップ 2: IAMグループを作成してポリシーをアタッチする

IAM 管理者は、グループを作成し、作成したポリシーをグループにアタッチできます。IAM ユーザーはいつでもグループに追加できます。

IAM グループを作成してポリシーをアタッチするには

1. ナビゲーションペインで、[Groups]、[Create New Group] の順に選択します。
2. [グループ名] にグループの名前を入力し、[次のステップ] を選択します。
3. 作成したポリシーの名前を検索ボックスに入力します。 ポリシーのチェックボックスを選択にし、[次のステップ] を選択します。

4. グループ名とポリシーを確認します。準備ができたら、[グループの作成] を選択します。

ステップ 3: IAM ユーザーを作成し、グループに追加する

IAM 管理者は、ユーザーをいつでもグループに追加できます。ユーザーを追加すると、グループに付与された権限がユーザーに付与されます。

IAM ユーザーを作成し、そのユーザーをグループに追加するには

1. ナビゲーションペインで、[Users] (ユーザー)、[Add user] (ユーザーを追加する) の順に選択します。
2. [ユーザー名] に 1 人または複数のユーザーの名前を入力します。
3. AWS Management Console アクセス の横にあるチェックボックスを選択します。自動生成されたパスワードまたはカスタムパスワードを設定します。必要に応じて、[ーザーは次回のサインインで新しいパスワードを作成する必要があります] を選択して、初回サインイン時にパスワードのリセットを要求できます。
4. [Next: Permissions] (次へ: アクセス許可) を選択します。
5. [ユーザーをグループに追加] をクリックし、作成したグループを選択します。
6. [Next: Tags] (次へ: タグ) を選択します。必要に応じて、ユーザーにタグを追加できます。
7. [次へ: レビュー] を選択します。準備が完了したら、[ユーザーの作成] を選択します。

のきめ細かなアクセス許可へのレポートの移行 AWS Artifact

きめ細かなアクセス許可を使用できるようになりました AWS Artifact。これらのきめ細かなアクセス許可により、用語の受け入れやレポートのダウンロードなどの機能へのアクセスをきめ細かく制御できます。

きめ細かなアクセス許可を使用してレポートにアクセスするには、AWSArtifactReportsReadOnlyAccess 管理ポリシーを使用するか、以下の推奨事項に従ってアクセス許可を更新できます。以前にきめ細かなアクセス許可の使用をオプトアウトしたことがある場合は、レポートコンソールで利用可能なAWS「Artifact レポートのきめ細かなアクセス許可へのオプトイン」リンクを使用してオプトインする必要があります。

新しいアクセス許可の更新に問題がある場合は、コンソールで利用可能なAWS「アーティファクトレポートのきめ細かなアクセス許可のオプトアウト」リンクから、古いアクセス許可を持つレポートにアクセスできます。

レポートを新しいアクセス許可に移行する

リソース固有以外のアクセス許可の移行

レガシーアクセス許可を含む既存のポリシーを、きめ細かなアクセス許可を含むポリシーに置き換えます。

レガシーポリシー：

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

きめ細かなアクセス許可を持つ新しいポリシー：

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

リソース固有の権限の移行

レガシーアクセス許可を含む既存のポリシーを、きめ細かなアクセス許可を含むポリシーに置き換えます。レポートリソースのワイルドカード権限は条件キーに置き換えられました。

レガシーポリシー：

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

きめ細かなアクセス許可と条件キーを持つ新しいポリシー：

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

AWS アーティファクト契約のきめ細かなアクセス許可への移行

AWS Artifact では、契約にきめ細かなアクセス許可を使用できるようになりました。これらのきめ細かなアクセス許可により、お客様は、機密保持契約の表示と受諾、契約の受諾と終了などの機能へのアクセスをきめ細かく制御できます。

きめ細かなアクセス許可を使用して契約にアクセスするには、AWSArtifactAgreementsReadOnlyAccess または AWSArtifactAgreementsFullAccess 管理ポリシーを使用するか、以下の推奨事項に従ってアクセス許可を更新できます。以前にきめ細かなアクセス許可の使用をオプトアウトしたことがある場合は、契約コンソールで利用可能なAWS「アーティファクト契約のきめ細かなアクセス許可へのオプトイン」リンクを使用してオプトインする必要があります。

新しいアクセス許可の更新に問題がある場合は、コンソールで利用可能なAWS「アーティファクト契約のきめ細かなアクセス許可のオプトアウト」リンクから、古いアクセス許可を持つ契約にアクセスできます。

新しい権限への移行

レガシーIAMアクションDownloadAgreement「」は、承諾されていない契約をダウンロードするためのGetAgreement「」アクションと、承諾された契約をダウンロードするためのGetCustomerAgreement「」アクションに置き換えられました。さらに、非開示契約 () を表示および承諾するためのアクセスを制御するためのより詳細なアクションが導入されましたNDAs。これらの詳細なアクションを活用し、契約を表示および実行する機能を維持するには、ユーザーはレガシーアクセス許可を含む既存のポリシーを、きめ細かなアクセス許可を含むポリシーに置き換える必要があります。

アカウントレベルで契約をダウンロードするアクセス許可を移行する

従来のポリシー:

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

きめ細かい権限を持つ新しいポリシー:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:GetAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptNdaForAgreement"
      ],
      "Resource": [
```

```
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

アカウントレベルで契約をダウンロード、受諾、終了するためのリソース固有以外のアクセス許可を移行する

従来のポリシー:

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

きめ細かい権限を持つ新しいポリシー:

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
        "Sid": "ListAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:ListAgreements",
            "artifact:ListCustomerAgreements"
        ],
```

```
        "Resource": "*"
      },
      {
        "Sid": "AWSAgreementActions",
        "Effect": "Allow",
        "Action": [
          "artifact:GetAgreement",
          "artifact:AcceptNdaForAgreement",
          "artifact:GetNdaForAgreement",
          "artifact:AcceptAgreement"
        ],
        "Resource": "arn:aws:artifact:::agreement/*"
      },
      {
        "Sid": "CustomerAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:GetCustomerAgreement",
            "artifact:TerminateAgreement"
        ],
        "Resource": "arn:aws:artifact::*:customer-agreement/*"
      }
    ]
}
```

組織レベルで契約をダウンロード、受諾、終了するためのリソース固有以外のアクセス許可を移行する

従来のポリシー:

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

きめ細かい権限を持つ新しいポリシー:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
```

```
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
```

```
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

アカウントレベルで契約をダウンロード、受諾、終了するためのリソース固有のアクセス許可を移行する

従来のポリシー:

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

きめ細かい権限を持つ新しいポリシー:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

組織レベルで契約をダウンロード、受諾、終了するためのリソース固有のアクセス許可を移行する

従来のポリシー:

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

```
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/AWS Organizations Business Associate Addendum"
      ]
    },
    {
      "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": "*"
    }
  ]
}
```

きめ細かい権限を持つ新しいポリシー:

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

```
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

契約のレガシーからきめ細かなリソースマッピング

契約 ARNの は、きめ細かなアクセス許可のために更新されました。レガシー契約リソースへの以前の参照は、新しい ARNに置き換える必要があります。以下は、レガシーリソースときめ細かなリソース間の契約ARNマッピングです。

契約名	レガシーアクセス許可ARNのアーティファクト	きめ細かなアクセス許可ARNのアーティファクト
AWS 事業提携契約	arn:aws:artifact:::agreement/AWS Business Associate Addendum	arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm
AWS ニュージーランドの通知可能なデータ侵害に関する付録	arn:aws:artifact:::agreement/AWSNew Zealand Notifiable Data Breach Addendum	arn:aws:artifact:::agreement/agreement-3YRq9rGUIu72r7Gt

契約名	レガシーアクセス許可ARNのアーティファクト	きめ細かなアクセス許可ARNのアーティファクト
AWS オーストラリアの通知可能なデータ侵害に関する付録	arn:aws:artifact:::agreement/AWSAustralian Notifiable Data Breach Addendum	arn:aws:artifact:::agreement/agreement-sbLSDe8bitmAXNr9
AWS SEC ルール 17a-4 付録	arn:aws:artifact:::agreement/AWS SECルール 17a-4 付録	arn:aws:artifact:::agreement/agreement-bexgr7sjvXAW4Gxu
AWS SEC ルール 18a-6 付録	arn:aws:artifact:::agreement/AWS SECルール 18a-6 付録	arn:aws:artifact:::agreement/agreement-HZTdNwJuqOKLReXC
AWS Organizations 事業提携契約	arn:aws:artifact:::agreement/AWSOrganizations Business Associate Addendum	arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv
AWS Organizations オーストラリア通知可能データ侵害に関する付録	arn:aws:artifact:::agreement/AWSOrganizations オーストラリア通知可能データ侵害に関する付録	arn:aws:artifact:::agreement/agreement-YpDMFXTePE7kEg4b
AWS Organizations ニュージーランドの通知可能なデータ侵害に関する付録	arn:aws:artifact:::agreement/AWSOrganizations ニュージーランドの通知可能なデータ侵害に関する追加契約	arn:aws:artifact:::agreement/agreement-uojEjr3vOnvrhV52

のIAMポリシーの例 AWS Artifact

IAM ユーザーに許可を付与する許可ポリシーを作成できます。 AWS Artifact レポートへのアクセス権をユーザーに付与し、単一のアカウントまたは組織に代わって契約を受諾およびダウンロードすることができます。

次のポリシー例は、必要なアクセスレベルに基づいてIAMユーザーに割り当てることができるアクセス許可を示しています。

- きめ細かなアクセス許可で AWS レポートを管理するポリシーの例
- サードパーティレポートを管理するポリシーの例
- 契約を管理するポリシーの例
- と統合するポリシーの例 AWS Organizations
- 管理アカウントの契約を管理するポリシーの例
- 組織的な契約を管理するポリシーの例
- 通知を管理するポリシーの例

Example きめ細かなアクセス許可で AWS レポートを管理するポリシーの例

> **Tip**
>
> 独自のAWSArtifactReportsReadOnlyAccessポリシーを定義するのではなく、 管理ポリシーの使用を検討する必要があります。

次のポリシーは、きめ細かなアクセス許可を使用してすべての AWS レポートをダウンロードするアクセス許可を付与します。

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

次のポリシーは AWS SOC、きめ細かなアクセス許可を通じて、、PCI、および ISOレポートのみをダウンロードするアクセス許可を付与します。

```
{
  "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 サードパーティレポートを管理するポリシーの例

> **Tip**
>
> 独自のAWSArtifactReportsReadOnlyAccessポリシーを定義する代わりに、 管理ポリシーの使用を検討する必要があります。

サードパーティーのレポートは、IAMリソース によって示されますreport。

次のポリシーは、すべてのサードパーティレポート機能に対しアクセス許可を付与します。

```
{
```

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

次のポリシーは、サードパーティレポートをダウンロードするアクセス許可を付与します。

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

次のポリシーは、サードパーティレポートを一覧表示するアクセス許可を付与します。

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

```
  ]
}
```

次のポリシーは、すべてのバージョンに関するサードパーティーレポートの詳細を表示するアクセス許可を付与します。

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

次のポリシーは、特定のバージョンに関するサードパーティーレポートの詳細を表示するアクセス許可を付与します。

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

> **Tip**
>
> 独自のAWSArtifactAgreementsReadOnlyAccessポリシーを定義する代わりに、 またはAWSArtifactAgreementsFullAccess 管理ポリシーを使用することを検討してください。

Example 契約を管理するポリシーの例

次のポリシーは、すべての契約をダウンロードするアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
```

```
}
```

次のポリシーは、すべての契約を受諾するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
}
```

次のポリシーは、すべての契約を終了するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
```

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

次のポリシーは、アカウントレベル契約を表示および実行するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
```

```
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Example と統合するポリシーの例 AWS Organizations

次のポリシー AWS Artifact は、 が統合に使用する IAM ロールを作成するアクセス許可を付与します AWS Organizations。組織的な契約を開始するには、組織の管理アカウントにこれらのアクセス許可が必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

次のポリシーは、 を使用するアクセス許可を付与するアクセス許可を付与 AWS Artifact します AWS Organizations。組織的な契約を開始するには、組織の管理アカウントにこれらのアクセス許可が必要です。

```
{
```

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

Example 管理アカウントの契約を管理するポリシーの例

次のポリシーは、管理アカウントの契約を管理するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 組織的な契約を管理するポリシーの例

次のポリシーは、組織的な契約を管理するアクセス許可を付与します。必要な権限を持つ別のユーザーが組織的な契約を設定する必要があります。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

次のポリシーは、組織的な契約を表示するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 通知を管理するポリシーの例

次のポリシーは、 AWS Artifact 通知を使用するための完全なアクセス許可を付与します。

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

次のポリシーは、すべての設定を一覧表示するためのアクセス許可を付与します。

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

次のポリシーは、設定を作成するアクセス許可を付与します。

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

```
    }
  ]
}
```

次のポリシーは、設定を編集するアクセス許可を付与します。

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

次のポリシーは、設定を削除するアクセス許可を付与します。

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

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

次のポリシーは、設定の詳細を表示するアクセス許可を付与します。

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

次のポリシーは、通知ハブを登録または登録解除するアクセス許可を付与します。

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

```
      ]
    }
  ]
}
```

の AWS 管理ポリシーの使用 AWS Artifact

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 AWS AWS のサービス は、新しい が起動されたとき、または既存のサービスで新しいAPIオペレーションが利用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

AWS 管理ポリシー： AWSArtifactReportsReadOnlyAccess

`AWSArtifactReportsReadOnlyAccess` ポリシーを IAM ID にアタッチできます。

このポリシーは、レポートの一覧表示、表示、ダウンロードを許可する*`read-only`*アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `artifact` – プリンシパルがレポートを一覧表示、表示、ダウンロードできるようにします AWS Artifact。

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

AWS 管理ポリシー： AWSArtifactAgreementsReadOnlyAccess

AWSArtifactAgreementsReadOnlyAccess ポリシーを IAM ID にアタッチできます。

このポリシーは、AWSアーティファクトサービス契約を一覧表示し、受諾された契約をダウンロードする*read-only*アクセスを許可します。また、組織の詳細を一覧表示し、記述するアクセス許可も含まれています。さらに、このポリシーでは、必要なサービスにリンクされたロールが存在するかどうかを確認できます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- artifact – プリンシパルがすべての契約を一覧表示し、承諾された契約を表示できるようにします AWS Artifact。
- IAM — プリンシパルが を使用して、サービスにリンクされたロールが存在するかどうかをチェックできるようにします GetRole。
- organization – プリンシパルが組織を記述し、組織のサービスアクセスを一覧表示できるようにします。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetCustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "AWSOrganizationActions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

AWS 管理ポリシー： AWSArtifactAgreementsFullAccess

AWSArtifactAgreementsFullAccess ポリシーを IAM ID にアタッチできます。

このポリシーは、AWSアーティファクト契約を一覧表示、ダウンロード、承諾、終了する*full*アクセス許可を付与します。また、Organization サービスでAWSサービスアクセスを一覧表示して有効にするアクセス許可や、組織の詳細を記述するアクセス許可も含まれています。さらに、このポリシーでは、必要なサービスにリンクされたロールが存在するかどうかを確認し、存在しない場合はロールを作成します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `artifact` – プリンシパルが契約を一覧表示、ダウンロード、受諾、および終了できるようにします AWS Artifact。
- `IAM` – プリンシパルがサービスにリンクされたロールを作成し、 を使用してサービスにリンクされたロールが存在するかどうかをチェックできるようにします GetRole。
- `organization` – プリンシパルが組織を記述し、組織のサービスアクセスを一覧表示/有効化できるようにします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
```

```
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

AWS ArtifactAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AWS Artifact 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートを受け取るには、 AWS Artifact ドキュメント履歴ページのRSSフィードにサブスクライブします。

変更	説明	日付
AWS Artifact が変更の追跡を開始しました	AWS Artifact が AWS マネージドポリシーの変更の追跡を開始し、 を導入しました AWSArtifactReports ReadOnlyAccess。	2023-12-15
AWS 契約管理ポリシーを導入	ポリシー AWSArtifactAgreementsReadOnlyAccess と AWSArtifactAgreementsFullAccess 管理ポリシーを導入しました。	2024-11-21

AWS Artifactのサービスにリンクされたロールの使用

AWS Artifact は AWS Identity and Access Management （ IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 に直接リンクされる一意のタイプのIAMロールです AWS Artifact。サービスにリンクされたロールは によって事前定義 AWS Artifact され、ユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれます。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、設定 AWS Artifact が簡単になります。 は、サービスにリンクされたロールのアクセス許可 AWS Artifact を定義し、特に定義されていない限り、 AWS Artifact はロールのみを引き受けることができます。定義されたアクセス許可には、信頼ポリシーとアクセス許可ポリシーが含まれ、そのアクセス許可ポリシーを他のIAMエンティティにアタッチすることはできません。

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、 AWS Artifact リソースへのアクセス許可を誤って削除できないため、リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスの詳細については、AWS 「 と連携するIAMサービス」を参照してください。また、「サービスにリンクされたロール」列で「はい」のサービスを探します。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[Yes] (はい) リンクを選択します。

のサービスにリンクされたロールのアクセス許可 AWS Artifact

AWS Artifact は、 という名前のサービスにリンクされたロールを使用します。AWSServiceRoleForArtifact を使用して組織に関する情報を収集 AWS Artifact できます AWS Organizations。

AWSServiceRoleForArtifact サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `artifact.amazonaws.com`

という名前のロールアクセス許可ポリシー AWSArtifactServiceRolePolicy では AWS Artifact 、が`organizations`リソースに対して次のアクションを実行できます。

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

のサービスにリンクされたロールの作成 AWS Artifact

サービスにリンクされたロールを手動で作成する必要はありません。組織管理アカウントの Organization agreements タブに移動し、 で開始するリンクを選択すると AWS Management Console、 はサービスにリンクされたロール AWS Artifact を作成します。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。組織管理アカウントの Organization agreements タブに移動し、Get started リンクを選択すると、 はサービスにリンクされたロールを再度 AWS Artifact 作成します。

のサービスにリンクされたロールの編集 AWS Artifact

AWS Artifact では、 AWSServiceRoleForArtifact サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、 を使用してロールの説明を編集できますIAM。詳細については、 IAM ユーザーガイドの「サービスにリンクされたロールの編集」を参照してください。

のサービスにリンクされたロールの削除 AWS Artifact

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースの削除時に AWS Artifact サービスが ロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

で使用される AWS Artifact リソースを削除するには AWSServiceRoleForArtifact

1. AWS Artifact コンソールの「組織契約」テーブルにアクセスする
2. 有効な組織契約をすべて終了します。

を使用してサービスにリンクされたロールを手動で削除するには IAM

IAM コンソール、 AWS CLI、または AWS API を使用して、 AWSServiceRoleForArtifact サービスにリンクされたロールを削除します。詳細については、IAM「 ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

AWS Artifact サービスにリンクされたロールでサポートされているリージョン

AWS Artifact は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートしていません。 AWSServiceRoleForArtifact ロールは、次のリージョンで使用できます。

リージョン名	リージョン識別子	でのサポート AWS Artifact
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	なし
米国西部 (北カリフォルニア)	us-west-1	なし
米国西部 (オレゴン)	us-west-2	はい
アフリカ (ケープタウン)	af-south-1	いいえ
アジアパシフィック (香港)	ap-east-1	いいえ
アジアパシフィック (ジャカルタ)	ap-southeast-3	いいえ
アジアパシフィック (ムンバイ)	ap-south-1	なし
アジアパシフィック (大阪)	ap-northeast-3	いいえ
アジアパシフィック (ソウル)	ap-northeast-2	なし
アジアパシフィック (シンガポール)	ap-southeast-1	なし
アジアパシフィック (シドニー)	ap-southeast-2	なし
アジアパシフィック (東京)	ap-northeast-1	なし
カナダ (中部)	ca-central-1	なし
欧州 (フランクフルト)	eu-central-1	なし
欧州 (アイルランド)	eu-west-1	なし
欧州 (ロンドン)	eu-west-2	なし
欧州 (ミラノ)	eu-south-1	いいえ
欧州 (パリ)	eu-west-3	なし
欧州 (ストックホルム)	eu-north-1	なし

リージョン名	リージョン識別子	でのサポート AWS Artifact
中東 (バーレーン)	me-south-1	なし
中東 (UAE)	me-central-1	なし
南米 (サンパウロ)	sa-east-1	なし
AWS GovCloud （米国東部）	us-gov-east-1	なし
AWS GovCloud （米国西部）	us-gov-west-1	なし

AWS Artifact レポートのIAM条件キーの使用

IAM 条件キーを使用して、特定のレポートカテゴリとシリーズに基づいて AWS Artifact、 のレポートへのきめ細かなアクセスを提供できます。

次のポリシーの例は、特定のレポートカテゴリとシリーズに基づいてIAMユーザーに割り当てることができるアクセス許可を示しています。

Example AWS レポートの読み取りアクセスを管理するポリシーの例

AWS Artifact レポートはIAMリソース によって示されます`report`。

次のポリシーは、`Certifications and Attestations`カテゴリ内のすべての AWS Artifact レポートを読み取るアクセス許可を付与します。

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

次のポリシーでは、SOCシリーズ内のすべての AWS Artifact レポートを読み取るアクセス許可を付与できます。

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

```
    ]
}
```

次のポリシーでは、Certifications and Attestationsカテゴリ内のレポートを除くすべての AWS Artifact レポートを読み取るアクセス許可を付与できます。

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

を使用した呼び出しのログ記録 AWS Artifact API AWS CloudTrail

AWS Artifact は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています AWS Artifact。 CloudTrail キャプチャでは、 をイベント AWS Artifact としてAPI呼び出します。キャプチャされた呼び出しには、AWS Artifact コンソールからの呼び出しと、 オペレーションへのコード呼び出しが含まれます AWS Artifact API。証跡を作成する場合は、 CloudTrail イベントを含む Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます AWS Artifact。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、リクエストの実行元の IP アドレス AWS Artifact、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。

詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

AWS Artifact の情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 は で有効になります。でアクティビティが発生すると AWS Artifact、そのアクティビティは CloudTrail イベント履歴の他の AWS サービスイベントとともにイベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

のイベントなど AWS アカウント、 のイベントの継続的な記録については AWS Artifact、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- CloudTrail がサポートするサービスと統合
- の Amazon SNS通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

AWS Artifact では、以下のアクションをイベントとして CloudTrail ログファイルに記録できます。

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings
- AcceptAgreement
- AcceptNdaForAgreement
- GetAgreement
- GetCustomerAgreement
- GetNdaForAgreement
- ListAgreements
- ListCustomerAgreements
- TerminateAgreement

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストが root または AWS Identity and Access Management（IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、 CloudTrail userIdentity要素を参照してください。

AWS Artifact ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパ

ラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリックAPIコールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 GetReportMetadata アクションを示す CloudTrail ログエントリを示しています。


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

のドキュメント履歴 AWS Artifact

次の表は、 AWS Artifact ユーザーガイドの AWS Artifact リリースおよび関連する変更の履歴を示しています。

変更	説明	日付
契約実行 AWSArtifactAgreementsFullAccess と AWSArtifactAgreementsReadOnlyAccess 管理ポリシーのためのきめ細かなアクセス許可	AWS Artifact 契約実行と起動AWSArtifactAgreementsFullAccess AWSArtifactAgreementsReadOnlyAccess AWS および管理ポリシーのきめ細かなアクセスを有効にしました。	2024 年 11 月 21 日
きめ細かなレポートアクセスと AWSArtifactReportReadOnlyAccess 管理ポリシー	AWS Artifact レポートへのきめ細かなアクセスを有効にし、レポート条件キーを有効にし、AWSArtifactReportsReadOnlyAccess管理ポリシーを起動しました。	2023 年 12 月 15 日
AWS Artifact サービスにリンクされたロール	サービスにリンクされたロールのドキュメントを追加し、AWS Artifact および AWS Organizations 統合のポリシー例を更新しました。	2023 年 9 月 26 日
通知	通知の管理に関するドキュメントを公開し、 リファレンス、 CloudTrail ログ記録ドキュメント、および Identity and Access Management ページに関連する AWS Artifact API更新を行いました。	2023 年 8 月 1 日

「サードパーティレポート - 一般提供を開始」	API リファレンスドキュメントと CloudTrail ログ記録ドキュメントを追加し、サードパーティーのレポートを一般公開しました。	2023 年 1 月 27 日
「サードパーティレポート (プレビュー)」	製品を販売する独立系ソフトウェアベンダー (ISVs) のコンプライアンスレポートを起動しました AWS Marketplace。サードパーティーレポートの Identity and Access Management ページにポリシーの例を追加しました。	2022 年 11 月 30 日
セキュリティ	「混乱した代理」防止のための「アイデンティティとアクセス管理」ページにセクションを追加しました。	2021 年 12 月 20 日
レポート	機密保持契約を削除し、レポートのダウンロードに関する利用規約を導入しました。	2020 年 12 月 17 日
ホームページと検索	レポートと契約ページにサービスホームページと検索バーを追加しました。	2020 年 5 月 15 日
GovCloud 起動	AWS Artifact で起動しました AWS GovCloud (US) Regions。	2019 年 11 月 7 日
AWS Organizations 契約	組織の契約の管理に関するサポートを追加しました。	2018 年 6 月 20 日
契約	AWS Artifact 契約管理のサポートを追加しました。	2017 年 6 月 17 日

初回リリース	このリリースでは AWS Artifactを導入しています。	2016 年 11 月 30 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。