Guide de l’utilisateur

AWS Artifact

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Artifact: Guide de l’utilisateur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que c'est AWS Artifact ?

AWS Artifact fournit des téléchargements à la demande de documents de AWS sécurité et de conformité. Par exemple, des rapports sur la conformité aux normes de l'Organisation internationale de normalisation (ISO) et aux normes de sécurité de l'industrie des cartes de paiement (PCI), ainsi que des rapports sur les contrôles du système et de l'organisation (SOC). AWS Artifact fournit également des téléchargements de certifications émanant d'organismes d'accréditation qui valident la mise en œuvre et l'efficacité opérationnelle des contrôles de AWS sécurité.

Avec AWS Artifact, vous pouvez également télécharger des documents de sécurité et de conformité pour les fournisseurs de logiciels indépendants (ISVs) qui vendent leurs produits sur AWS Marketplace. Pour plus d'informations, consultez AWS Marketplace Vendor Insights.

En outre, vous pouvez l'utiliser AWS Artifact pour consulter, accepter et suivre le statut de vos accords avec AWS vous Compte AWS et pour plusieurs membres Comptes AWS de votre organisation. Pour plus d'informations sur les accords conclus dans AWS Artifact, voirGestion des accords dans AWS Artifact.

Pour démontrer la sécurité et la conformité de l' AWS infrastructure et des services que vous utilisez, vous pouvez soumettre AWS Artifact des documents à vos auditeurs ou régulateurs sous forme d'artefacts d'audit. Vous pouvez également utiliser ces artefacts d'audit comme directives pour évaluer votre propre architecture cloud et pour évaluer l'efficacité des contrôles internes de votre entreprise. Pour plus d'informations sur les artefacts d'audit, consultez AWS Artifact FAQs.

> **Note**
>
> AWS les clients sont responsables de l'élaboration ou de l'obtention de documents démontrant la sécurité et la conformité de leurs entreprises. Pour plus d'informations, consultez Modèle de responsabilité partagée.

Tarification

AWS vous fournit des AWS Artifact documents et des accords gratuitement.

Commencer avec AWS Artifact

Pour commencer à l'utiliser AWS Artifact, testez ses principales fonctionnalités dans la AWS Artifact console. Dans la console, vous pouvez télécharger des rapports AWS de sécurité et de conformité, télécharger et accepter des accords juridiques, et vous abonner aux notifications relatives aux AWS Artifact documents.

Prérequis

Pour utiliser les fonctionnalités de AWS Artifact, vous devez disposer d'un Compte AWS. Pour les instructions de configuration, voir Configurer un nouveau Compte AWS dans le Guide de l'utilisateur d'AWS installation.

Fonctionnalités

Pour obtenir des instructions sur l'utilisation des fonctionnalités de AWS Artifact, consultez les rubriques suivantes :

- Téléchargement de rapports
- Gestion des accords
- Configuration des notifications

Téléchargement de rapports dans AWS Artifact

Vous pouvez télécharger les rapports depuis la AWS Artifact console. Lorsque vous téléchargez un rapport depuis AWS Artifact, celui-ci est généré spécialement pour vous, et chaque rapport possède un filigrane unique. C'est pourquoi vous devez partager les rapports uniquement avec des personnes de confiance. N'envoyez pas ces rapports par e-mail sous forme de pièces jointes et ne les partagez pas en ligne. Pour partager un rapport, utilisez un service de partage sécurisé tel qu'Amazon WorkDocs. Certains rapports nécessitent que vous acceptiez les conditions générales avant de pouvoir les télécharger.

Table des matières

Téléchargement d'un rapport

Pour télécharger un rapport, vous devez disposer des autorisations requises. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans AWS Artifact.

Lorsque vous vous inscrivez AWS Artifact, votre compte est automatiquement autorisé à télécharger certains rapports. Si vous rencontrez des difficultés pour y accéder AWS Artifact, suivez les instructions sur la page de référence d'autorisation de AWS Artifact service.

Pour télécharger un rapport

1. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.
2. Sur la page d' AWS Artifact accueil, choisissez Afficher les rapports.

   Sur la page Rapports, dans l'onglet AWS Rapports, vous pouvez accéder aux AWS rapports (par exemple, SOC 1/2/3PCI, C5, etc.). Dans l'onglet Rapports tiers, vous pouvez accéder aux rapports des fournisseurs de logiciels indépendants (ISVs) sur lesquels ils vendent leurs produits AWS Marketplace.
3. (Facultatif) Pour trouver un rapport, entrez un mot clé dans le champ de recherche. Vous pouvez également effectuer des recherches ciblées pour les rapports en fonction de colonnes

individuelles, notamment le titre, la catégorie, la série et la description du rapport. Par exemple, pour trouver le rapport C5 (Cloud Computing Compliance Controls Catalogue), vous pouvez effectuer une recherche dans la colonne Titre en utilisant « Titre », l'opérateur « contient » (:)) et le terme « C5 » (**`Title : C5`**).

4. (Facultatif) Pour plus d'informations sur un rapport, choisissez le titre du rapport pour ouvrir sa page de détails.
5. Sélectionnez un rapport, puis choisissez Télécharger le rapport.
6. Vous serez peut-être invité à accepter les conditions générales (Accepter les conditions pour télécharger le rapport) pour le rapport spécifique que vous êtes en train de télécharger. Nous vous recommandons de lire attentivement les termes et conditions. Lorsque vous avez fini de lire, sélectionnez J'ai lu et j'accepte les conditions, puis choisissez Accepter les conditions et télécharger le rapport.
7. Ouvrez le fichier téléchargé via un PDF visualiseur. Consultez les conditions générales d'acceptation et faites défiler la page vers le bas pour trouver le rapport d'audit. Les rapports peuvent contenir des informations supplémentaires intégrées sous forme de pièces jointes au PDF document. Assurez-vous donc de vérifier la présence de pièces jointes dans le PDF fichier pour les pièces justificatives. Pour obtenir des instructions sur la façon d'afficher les pièces jointes, consultezAfficher les pièces jointes dans PDF les documents.

Afficher les pièces jointes dans PDF les documents

Nous recommandons les applications suivantes qui prennent actuellement en charge l'affichage des PDF pièces jointes :

Adobe Acrobat Reader

Téléchargez la dernière version d'Adobe Acrobat Reader sur le site Web d'Adobe à https://get.adobe.com/reader/l'adresse.

Pour obtenir des instructions sur la façon d'afficher PDF les pièces jointes dans Acrobat Reader, consultez la section Liens et pièces jointes PDFs sur le site Web de support d'Adobe.

Navigateur Firefox

1. Téléchargez le dernier navigateur Web Firefox sur le site Web de Mozilla à l'adresse https://www.mozilla. org/en-US/firefox/new/.

2. Ouvrez le PDF fichier dans le PDF visualiseur intégré de Firefox. Pour obtenir des instructions, consultez Afficher PDF les fichiers dans Firefox ou choisissez un autre lecteur sur le site Web du Support de Mozilla.
3. Pour afficher les PDF pièces jointes dans le PDF visualiseur intégré de Firefox, choisissez Basculer dans la barre latérale, puis Afficher les pièces jointes.

Sécurisation de vos documents

AWS Artifact les documents sont confidentiels et doivent être conservés en lieu sûr en tout temps. AWS Artifact utilise le modèle de responsabilité AWS partagée pour ses documents. Cela signifie qu'il AWS est responsable de la sécurité des documents lorsqu'ils sont dans le AWS cloud, mais que vous êtes responsable de leur sécurité une fois que vous les avez téléchargés. AWS Artifact peut vous obliger à accepter les conditions générales avant de pouvoir télécharger des documents. Chaque téléchargement de document est associé à un filigrane traçable unique.

Vous êtes uniquement autorisé à partager des documents marqués comme confidentiels au sein de votre entreprise, avec vos régulateurs et avec vos auditeurs. Vous n'êtes pas autorisé à partager ces documents avec vos clients ou sur votre site web. Nous vous recommandons vivement d'utiliser un service de partage de documents sécurisé, tel qu'Amazon WorkDocs, pour partager des documents avec d'autres personnes. N'envoyez pas les documents par e-mail et ne les téléchargez pas sur un site non sécurisé.

Résolution des problèmes

Si vous ne parvenez pas à télécharger un document ou si vous recevez un message d'erreur, consultez la section Résolution des problèmes dans le AWS Artifact FAQ.

Gestion des accords dans AWS Artifact

Vous pouvez l'utiliser AWS Artifact pour examiner et gérer les accords pour votre entreprise Compte AWS ou celle de votre organisation. Par exemple, les entreprises soumises à la Health Insurance Portability and Accountability Act (HIPAA) ont généralement besoin d'un accord Business Associate Addendum (BAA) AWS pour garantir que les informations de santé protégées (PHI) sont protégées de manière appropriée. Dans la AWS Artifact console, vous pouvez consulter et accepter de tels accords, et vous pouvez en désigner un Compte AWS qui peut être légalement traitéPHI.

Si vous l'utilisez AWS Organizations, vous pouvez accepter des accords, tels qu'un accord BAA avec AWS, au nom de tous Comptes AWS les membres de votre organisation. Tous les comptes de membres existants et suivants sont automatiquement couverts par l'accord et peuvent être traités légalementPHI.

Vous pouvez également l'utiliser AWS Artifact pour confirmer que vous Compte AWS ou votre organisation avez accepté un accord, et pour examiner les termes d'un accord accepté afin de comprendre vos obligations. Si votre compte ou votre organisation n'a plus besoin d'utiliser un accord accepté, vous pouvez l'utiliser AWS Artifact pour le résilier. Si vous résiliez le contrat mais que vous vous rendez compte par la suite que vous en avez besoin, vous pouvez le réactiver.

Table des matières

Accepter des accords pour votre Compte AWS compte AWS Artifact

Vous pouvez utiliser la AWS Artifact console pour consulter et accepter des accords avec AWS for your Compte AWS.

> **Important**
>
> Avant d'accepter un accord, nous vous recommandons de consulter votre équipe en charge des aspects juridiques, de confidentialité et de conformité.

Autorisations nécessaires

Si vous êtes administrateur d'un compte, vous pouvez accorder IAM aux utilisateurs et aux utilisateurs fédérés les autorisations nécessaires pour accéder à un ou plusieurs de vos accords et les gérer. Par défaut, seuls les utilisateurs disposant de privilèges d'administrateurs peuvent accepter un accord. Pour accepter un accord, IAM les utilisateurs fédérés doivent disposer des autorisations requises.

Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans AWS Artifact.

Pour accepter un accord avec AWS

1. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.
2. Dans le volet AWS Artifact de navigation, sélectionnez Accords.
3. Choisissez l'onglet Account agreements (Accords de compte).
4. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.
5. Dans le volet de navigation, sélectionnez Accords.
6. Sur la page Accords, effectuez l'une des opérations suivantes :
   - Pour accepter un accord uniquement pour votre compte, cliquez sur l'onglet Accords relatifs au compte.
   - Pour accepter un accord au nom de votre organisation, cliquez sur l'onglet Accords d'organisation.
7. Sélectionnez un accord, puis choisissez Télécharger l'accord.

   La boîte NDAde dialogue Accepter de télécharger le rapport apparaît.
8. Avant de télécharger l'accord que vous avez sélectionné, vous devez d'abord accepter les termes de l'accord AWS Artifact de confidentialité (AWS Artifact NDA).

   a. Dans la boîte de dialogue NDAAccepter de télécharger le rapport, consultez le AWS Artifact NDA.

   b. (Facultatif) Pour imprimer une copie du AWS Artifact NDA (ou pour l'enregistrer en tant quePDF), choisissez Imprimer NDA.
   c. Sélectionnez J'ai lu et j'accepte toutes les conditions duNDA.
   d. Pour accepter le contrat que vous avez sélectionné AWS Artifact NDA et pour en télécharger unPDF, choisissez Accepter NDA et télécharger.
9. Dans un PDF lecteur, passez en revue le contrat PDF que vous avez téléchargé.
10. Dans la AWS Artifact console, après avoir sélectionné l'accord, choisissez Accepter l'accord.
11. Dans la boîte de dialogue Accepter l'accord, procédez comme suit :
    a. Passez en revue le contrat.
    b. Sélectionnez J'accepte tous ces termes et conditions.
    c. Choisissez Accepter l'accord.
12. Choisissez Accepter pour accepter l'accord relatif à votre compte.

Résiliation des contrats pour votre compte Compte AWSAWS Artifact

Si vous avez utilisé la AWS Artifact console pour accepter un accord pour un single Compte AWS, vous pouvez utiliser la console pour résilier cet accord. Sinon, consultez Contrats hors ligne dans AWS Artifact.

Autorisations nécessaires

Pour résilier un accord, IAM les utilisateurs fédérés doivent disposer des autorisations requises.

Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans AWS Artifact.

Pour résilier votre contrat en ligne avec AWS

1. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.
2. Dans le volet AWS Artifact de navigation, sélectionnez Accords.
3. Choisissez l'onglet Account agreements (Accords de compte).
4. Sélectionnez le contrat, puis cliquez sur Résilier le contrat.
5. Cochez toutes les cases pour indiquer que vous acceptez de résilier le contrat.

6. Sélectionnez Résilier. Lorsque vous êtes invité à confirmer, choisissez Terminate (Mettre fin).

Acceptation des accords pour votre organisation en AWS Artifact

Si vous êtes le propriétaire du compte de gestion d'une AWS Organizations organisation, vous pouvez accepter un accord au AWS nom de tous les membres Comptes AWS de votre organisation.

> **Important**
>
> Avant d'accepter un accord, nous vous recommandons de consulter votre équipe en charge des aspects juridiques, de confidentialité et de conformité.

AWS Organizations propose deux ensembles de fonctionnalités : les fonctionnalités de facturation consolidée et toutes les fonctionnalités. AWS Artifact Pour l'utiliser dans votre organisation, l'organisation à laquelle vous appartenez doit être activée pour toutes les fonctionnalités. Si votre organisation est configurée uniquement pour la facturation consolidée, consultez la section Activation de toutes les fonctionnalités de votre organisation dans le Guide de AWS Organizations l'utilisateur.

Pour accepter ou résilier des accords d'organisation, vous devez être connecté au compte de gestion avec les AWS Artifact autorisations appropriées. Les utilisateurs de comptes membres dotés `organizations:DescribeOrganization` d'autorisations peuvent consulter les accords d'organisation acceptés en leur nom.

Pour plus d'informations, consultez la section Gestion des comptes dans une organisation AWS Organizations dans le Guide de AWS Organizations l'utilisateur.

Autorisations nécessaires

Pour accepter un accord, le propriétaire du compte de gestion doit disposer des autorisations requises.

Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans AWS Artifact.

Pour accepter un accord pour votre organisation

1. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.
2. Sur le AWS Artifact tableau de bord, sélectionnez Accords.

3. Choisissez l'onglet Organization agreements (Accords d'organisation).
4. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.
5. Dans le volet de navigation, sélectionnez Accords.
6. Sur la page Accords, effectuez l'une des opérations suivantes :
   - Pour accepter un accord uniquement pour votre compte, cliquez sur l'onglet Accords relatifs au compte.
   - Pour accepter un accord au nom de votre organisation, cliquez sur l'onglet Accords d'organisation.
7. Sélectionnez un accord, puis choisissez Télécharger l'accord.

   La boîte NDAde dialogue Accepter de télécharger le rapport apparaît.
8. Avant de télécharger l'accord que vous avez sélectionné, vous devez d'abord accepter les termes de l'accord AWS Artifact de confidentialité (AWS Artifact NDA).

   a. Dans la boîte de dialogue NDAAccepter de télécharger le rapport, consultez le AWS Artifact NDA.

   b. (Facultatif) Pour imprimer une copie du AWS Artifact NDA (ou pour l'enregistrer en tant quePDF), choisissez Imprimer NDA.

   c. Sélectionnez J'ai lu et j'accepte toutes les conditions duNDA.

   d. Pour accepter le contrat que vous avez sélectionné AWS Artifact NDA et pour en télécharger unPDF, choisissez Accepter NDA et télécharger.
9. Dans un PDF lecteur, passez en revue le contrat PDF que vous avez téléchargé.
10. Dans la AWS Artifact console, après avoir sélectionné l'accord, choisissez Accepter l'accord.
11. Dans la boîte de dialogue Accepter l'accord, procédez comme suit :

    a. Passez en revue le contrat.

    b. Sélectionnez J'accepte tous ces termes et conditions.

    c. Choisissez Accepter l'accord.
12. Choisissez Accepter pour accepter l'accord pour tous les comptes existants et futurs de votre organisation.

Résiliation des contrats de votre organisation dans AWS Artifact

Si vous avez utilisé la AWS Artifact console pour accepter un accord au nom de tous les comptes membres d'une organisation dans AWS Organizations, vous pouvez utiliser la console pour résilier cet accord. Sinon, consultez Contrats hors ligne dans AWS Artifact.

Si le compte d'un membre est supprimé d'une organisation, ce compte de membre est plus couvert par les accords d'organisation. Avant de supprimer des comptes membres d'une organisation, un administrateur de comptes de gestion doit le communiquer aux comptes membres afin qu'ils puissent mettre en place de nouveaux accords si nécessaire. Vous pouvez consulter la liste des accords d'organisation actifs dans la AWS Artifact console sur la page Accords, sous Accords d'organisation.

Pour plus d'informations AWS Organizations, consultez la section Gestion des comptes dans une organisation AWS Organizations dans le Guide de AWS Organizations l'utilisateur.

Autorisations nécessaires

Pour résilier un accord, le propriétaire du compte de gestion doit disposer des autorisations requises.

Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans AWS Artifact.

Pour résilier votre contrat d'organisation en ligne avec AWS

1. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.
2. Sur le AWS Artifact tableau de bord, sélectionnez Accords.
3. Choisissez l'onglet Organization agreements (Accords d'organisation).
4. Sélectionnez le contrat, puis cliquez sur Résilier le contrat.
5. Cochez toutes les cases pour indiquer que vous acceptez de résilier le contrat.
6. Sélectionnez Résilier. Lorsque vous êtes invité à confirmer, choisissez Terminate (Mettre fin).

Contrats hors ligne dans AWS Artifact

Si vous avez un accord hors ligne existant, AWS Artifact affiche les accords que vous avez acceptés hors ligne. Par exemple, la console peut afficher l'addendum Offline Business Associate (BAA) avec le statut Actif. L'état actif indique que l'accord a été accepté. Pour résilier l'accord en ligne, consultez les directives et instructions de résiliation incluses dans votre accord.

Si votre compte est le compte de gestion d'une AWS Organizations organisation, vous pouvez l'utiliser AWS Artifact pour appliquer les termes de votre accord hors ligne à tous les comptes de votre organisation. Pour appliquer un accord que vous avez accepté hors ligne à votre organisation et à tous les comptes de votre organisation, vous devez disposer des autorisations requises.

Si votre compte est un compte membre d'une organisation, vous devez être autorisé à consulter vos accords d'organisation hors ligne.

Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans AWS Artifact.

Configuration des notifications par e-mail dans AWS Artifact

Vous pouvez utiliser la AWS Artifact console pour configurer les notifications par e-mail pour les mises à jour des accords et des rapports AWS Artifact. AWS Artifact envoie ces notifications par e-mail à l'aide de Notifications des utilisateurs AWS. Pour recevoir des notifications AWS Artifact par e-mail, vous devez d'abord sélectionner les hubs de Notifications des utilisateurs AWS notifications dans la Notifications des utilisateurs console. Ensuite, dans la AWS Artifact console, vous pouvez créer une configuration pour les paramètres de notification, dans laquelle vous spécifiez les destinataires des notifications et les notifications qu'ils reçoivent.

Pour configurer les notifications AWS Artifact par e-mail, vous devez disposer des autorisations requises pour AWS Artifact et Notifications des utilisateurs AWS. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans AWS Artifact.

Table des matières

Prérequis : sélectionnez les hubs de notification dans Notifications des utilisateurs

Avant de recevoir des notifications AWS Artifact par e-mail, vous devez d'abord ouvrir la Notifications des utilisateurs console et sélectionner les hubs de notification dans Régions AWS lesquels vous souhaitez stocker vos Notifications des utilisateurs données. La sélection de hubs de notification est requise pour Notifications des utilisateurs AWS, qui est AWS Artifact utilisé pour envoyer des notifications.

Pour sélectionner des hubs de notification

1. Ouvrez la page Notification Hubs de la Notifications des utilisateurs AWS console.
2. Sélectionnez les hubs de notification dans Régions AWS lesquels vous souhaitez stocker vos Notifications des utilisateurs AWS ressources. Par défaut, vos Notifications des utilisateurs données sont stockées dans la région USA Est (Virginie du Nord). Notifications des utilisateurs

réplique les données de vos notifications dans les autres régions que vous sélectionnez. Pour plus d'informations, consultez la documentation relative aux centres de notification dans le guide de Notifications des utilisateurs AWS l'utilisateur.

3. Choisissez Save and continue (Enregistrer et continuer).

Création d'une configuration pour les paramètres AWS Artifact de notification

Après avoir sélectionné vos hubs de Notifications des utilisateurs notification, vous pouvez créer une configuration pour les paramètres de notification dans la AWS Artifact console. Dans la configuration que vous créez, vous spécifiez les adresses e-mail des destinataires auxquels vous souhaitez recevoir des AWS Artifact notifications. Vous spécifiez également les mises à jour pour lesquelles les destinataires doivent recevoir des notifications, telles que les mises à jour des AWS Artifact accords et les mises à jour de tous les rapports (ou d'un sous-ensemble de) AWS Artifact rapports.

Pour créer une configuration

1. Ouvrez la page des paramètres de notification de la AWS Artifact console.
2. Choisissez Create configuration (Créer une configuration).
3. Sur la page Créer une configuration, procédez comme suit :
   - Pour recevoir des notifications relatives aux accords, sous Contrats, sélectionnez Mises à jour AWS des accords.
   - Pour recevoir des notifications relatives aux rapports, sous Rapports, maintenez l'option Mises à jour AWS des rapports sélectionnée.
     a. Pour recevoir des notifications pour tous les rapports, sélectionnez Tous les rapports.
     b. Pour recevoir des notifications uniquement pour les rapports appartenant à des catégories et séries spécifiques, choisissez Un sous-ensemble de rapports. Sélectionnez ensuite les catégories et les séries qui vous intéressent.
   - Sous Nom de la configuration, entrez le nom de votre configuration.
   - Sous E-mail, pour Destinataires, entrez une liste séparée par des virgules des adresses e-mail auxquelles vous souhaitez recevoir des e-mails de AWS Artifact notification.
   - (Facultatif) Pour ajouter des balises à la configuration des notifications, développez Tags, choisissez Ajouter une nouvelle balise, puis entrez les balises sous forme de paires clé-valeur. Pour plus d'informations sur le balisage Notifications des utilisateurs des ressources,

consultez la section Marquage de vos Notifications des utilisateurs AWS ressources dans le guide de l'Notifications des utilisateurs AWS utilisateur.

- Choisissez Create configuration (Créer une configuration).

  Notifications des utilisateurs envoie un e-mail de vérification à chacune des adresses e-mail des destinataires que vous avez fournies. Pour vérifier l'adresse e-mail, dans l'e-mail de vérification, le destinataire doit sélectionner Vérifier l'adresse e-mail. Seules les adresses e-mail vérifiées recevront des AWS Artifact notifications.

Modification d'une configuration pour les paramètres AWS Artifact de notification

Après avoir créé une configuration pour les paramètres de AWS Artifact notification, vous pouvez modifier la configuration à tout moment pour modifier vos paramètres de notification. Par exemple, pour ajouter ou supprimer des destinataires, modifier les types de notifications qu'ils reçoivent et ajouter ou supprimer des balises.

Pour modifier une configuration

1. Ouvrez la page des paramètres de notification de la AWS Artifact console.
2. Sélectionnez la configuration que vous souhaitez modifier.
3. Choisissez Modifier.
4. Modifiez les sélections et les champs de configuration. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

   Si vous avez ajouté de nouvelles adresses e-mail en tant que destinataires des notifications, Notifications des utilisateurs AWS envoyez un e-mail de vérification à ces adresses e-mail. Pour vérifier l'adresse e-mail, dans l'e-mail de vérification, le destinataire doit sélectionner Vérifier l'adresse e-mail. Seules les adresses e-mail vérifiées recevront des AWS Artifact notifications.

Supprimer une configuration pour les paramètres AWS Artifact de notification

Si vous n'avez plus besoin de la configuration que vous avez créée pour les paramètres de AWS Artifact notification, vous pouvez la supprimer dans la AWS Artifact console.

Pour supprimer une configuration

1. Ouvrez la page des paramètres de notification de la AWS Artifact console.
2. Sélectionnez la configuration que vous souhaitez supprimer.
3. Sélectionnez Delete (Supprimer).
4. Dans la boîte de dialogue Supprimer la configuration, choisissez Supprimer.

Gestion des identités et des accès dans AWS Artifact

Lorsque vous vous inscrivez AWS, vous fournissez une adresse e-mail et un mot de passe associés à votre AWS compte. Il s'agit de vos informations d'identification root, qui fournissent un accès complet à toutes vos AWS ressources, y compris aux ressources pour AWS Artifact. Cependant, nous vous conseillons vivement d'utiliser le compte racine pour un accès quotidien. Nous vous recommandons également de ne pas partager vos informations d'identification de compte avec d'autres personnes afin de leur donner un accès complet à votre compte.

Au lieu de vous connecter à votre AWS compte avec des informations d'identification root ou de partager vos informations d'identification avec d'autres personnes, vous devez créer une identité d'utilisateur spéciale appelée IAMutilisateur pour vous-même et pour toute personne susceptible d'avoir besoin d'accéder à un document ou à un accord AWS Artifact. Avec cette approche, vous pouvez fournir des informations de connexion individuelles à chaque utilisateur et vous pouvez accorder à chaque utilisateur uniquement les autorisations dont il a besoin pour utiliser certains documents. Vous pouvez également accorder les mêmes autorisations à plusieurs utilisateurs IAM en accordant ces autorisations à un groupe IAM, et en ajoutant les utilisateurs IAM à ce groupe.

Si vous gérez déjà les identités des utilisateurs en externe AWS, vous pouvez utiliser des fournisseurs IAM d'identité au lieu de créer des IAM utilisateurs. Pour plus d'informations, consultez la section Fournisseurs d'identité et fédération dans le guide de IAM l'utilisateur.

Table des matières

Octroi d'un accès utilisateur à AWS Artifact

Procédez comme suit pour accorder aux utilisateurs des autorisations en AWS Artifact fonction du niveau d'accès dont ils ont besoin.

Tâches

Étape 1 : Créer une stratégie IAM

En tant qu'IAMadministrateur, vous pouvez créer une politique qui accorde des autorisations aux AWS Artifact actions et aux ressources.

Pour créer une stratégie IAM

Utilisez la procédure suivante pour créer une IAM politique que vous pouvez utiliser pour accorder des autorisations à vos IAM utilisateurs et à vos groupes.

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Politiques.
3. Sélectionnez Create policy (Créer une politique).
4. Choisissez l'JSONonglet.
5. Entrez un document de politique. Vous pouvez créer votre propre politique ou utiliser l'une des politiques deExemples IAM de politiques pour AWS Artifact.
6. Choisissez Examiner une politique. Le programme de validation des politiques signale les éventuelles erreurs de syntaxe.
7. Sur la page Réviser la politique, entrez un nom unique qui vous aidera à vous souvenir de l'objectif de la politique. Vous pouvez également fournir une description.
8. Choisissez Create Policy (Créer une politique).

Étape 2 : créer un IAM groupe et joindre la politique

En tant IAM qu'administrateur, vous pouvez créer un groupe et y associer la politique que vous avez créée. Vous pouvez ajouter IAM des utilisateurs au groupe à tout moment.

Pour créer un IAM groupe et y associer votre politique

1. Dans le panneau de navigation, choisissez Groupes, puis Créer un nouveau groupe.
2. Dans Nom du groupe, entrez le nom de votre groupe, puis choisissez Next Step.

3. Dans le champ de recherche, entrez le nom de la politique que vous avez créée. Cochez la case correspondant à votre politique, puis choisissez Next Step.
4. Vérifiez le nom du groupe et les stratégies. Lorsque vous êtes prêt, choisissez Create Group.

Étape 3 : créer des IAM utilisateurs et les ajouter au groupe

En tant IAM qu'administrateur, vous pouvez ajouter des utilisateurs à un groupe à tout moment. Cela accorde aux utilisateurs les autorisations accordées au groupe.

Pour créer un IAM utilisateur et l'ajouter à un groupe

1. Dans le panneau de navigation, choisissez Utilisateurs, puis Add user (Ajouter un utilisateur).
2. Dans Nom d'utilisateur, entrez les noms d'un ou de plusieurs utilisateurs.
3. Cochez la case à côté de AWS Management Console access (Accès àAWS Management Console). Configurez un mot de passe personnalisé ou généré automatiquement. Vous pouvez éventuellement sélectionner L'utilisateur doit créer un nouveau mot de passe à la prochaine connexion pour demander une réinitialisation du mot de passe lors de la première connexion de l'utilisateur.
4. Sélectionnez Next: Permissions (Étape suivante : autorisations).
5. Choisissez Ajouter un utilisateur au groupe, puis sélectionnez le groupe que vous avez créé.
6. Choisissez Suivant : Balises. Vous pouvez éventuellement ajouter des tags à vos utilisateurs.
7. Choisissez Suivant : vérification. Lorsque vous êtes prêt, choisissez Create user.

Migration des rapports vers des autorisations détaillées pour AWS Artifact

Vous pouvez désormais utiliser des autorisations détaillées pour. AWS Artifact Grâce à ces autorisations détaillées, vous pouvez contrôler de manière précise l'accès à des fonctionnalités telles que l'acceptation des conditions et le téléchargement de rapports.

Pour accéder aux rapports via les autorisations détaillées, vous pouvez utiliser la politique AWSArtifactReportsReadOnlyAccessgérée ou mettre à jour vos autorisations conformément à la recommandation ci-dessous. Si vous avez précédemment choisi de ne pas utiliser les autorisations détaillées, vous devez vous inscrire en utilisant le lien « Accepter les autorisations détaillées pour les rapports AWS Artifact » disponible dans la console des rapports.

Vous avez la possibilité d'accéder aux rapports avec les anciennes autorisations via le lien « Désactiver les autorisations détaillées pour les rapports AWS Artifact » disponible dans la console en cas de problème lors de la mise à jour des nouvelles autorisations.

Migration des rapports vers de nouvelles autorisations

Migrer les autorisations non spécifiques aux ressources

Remplacez votre politique existante contenant des autorisations héritées par une politique contenant des autorisations détaillées.

Politique en matière d'héritage :

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

Nouvelle politique avec des autorisations détaillées :

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

Migrer les autorisations spécifiques aux ressources

Remplacez votre politique existante contenant des autorisations héritées par une politique contenant des autorisations détaillées. Les autorisations génériques des ressources de rapport ont été remplacées par des clés de condition.

Politique en matière d'héritage :

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

Nouvelle politique avec des autorisations et des clés de condition détaillées :

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

Migration vers des autorisations détaillées pour les accords Artifact AWS

AWSArtifact permet désormais aux clients d'utiliser des autorisations détaillées pour les accords. Grâce à ces autorisations détaillées, les clients disposent d'un contrôle précis sur l'accès à des fonctionnalités telles que la consultation et l'acceptation des accords de confidentialité, ainsi que l'acceptation et la résiliation des accords.

Pour accéder aux accords via les autorisations détaillées, vous pouvez utiliser les politiques AWSArtifactAgreementsReadOnlyAccessou les politiques AWSArtifactAgreementsFullAccess gérées ou mettre à jour vos autorisations conformément à la recommandation ci-dessous. Si vous avez précédemment choisi de ne pas utiliser d'autorisations détaillées, vous devez vous inscrire en utilisant le lien « Accepter les autorisations détaillées pour les accords AWS Artifact » disponible dans la console des accords.

Vous avez la possibilité d'accéder aux accords dotés d'anciennes autorisations via le lien « Désabonnement des autorisations détaillées pour les accords AWS Artifact » disponible dans la console en cas de problème lors de la mise à jour des nouvelles autorisations.

Migration vers de nouvelles autorisations

L'ancienne IAM action « DownloadAgreement » a été remplacée par l'action « GetAgreement » pour télécharger les accords non acceptés et par l'action « GetCustomerAgreement » pour télécharger les

accords acceptés. En outre, des actions plus détaillées ont été introduites pour contrôler l'accès à la consultation et à l'acceptation des accords de confidentialité ()NDAs. Pour tirer parti de ces actions granulaires et conserver la possibilité de consulter et d'exécuter les accords, les utilisateurs doivent remplacer leur politique existante contenant des autorisations héritées par une politique contenant des autorisations détaillées.

Migrer les autorisations pour télécharger le contrat au niveau du compte

Politique relative aux héritages :

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

Nouvelle politique avec des autorisations détaillées :

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

Migrer les autorisations non spécifiques aux ressources pour télécharger, accepter et résilier les accords au niveau du compte

Politique relative aux héritages :

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

Nouvelle politique avec des autorisations détaillées :

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

Migrer les autorisations non spécifiques aux ressources pour télécharger, accepter et résilier les accords au niveau de l'organisation

Politique relative aux héritages :

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

Nouvelle politique avec des autorisations détaillées :

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

Migrer les autorisations spécifiques aux ressources pour télécharger, accepter et résilier les accords au niveau du compte

Politique relative aux héritages :

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

Nouvelle politique avec des autorisations détaillées :

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

Migrer les autorisations spécifiques aux ressources pour télécharger, accepter et résilier les accords au niveau de l'organisation

Politique relative aux héritages :

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

```
}
```

Nouvelle politique avec des autorisations détaillées :

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

De l'héritage à une cartographie précise des ressources pour les accords

Les accords ARN ont été mis à jour pour des autorisations détaillées. Toute référence antérieure aux ressources des anciens accords doit être remplacée par ARN de nouvelles. Vous trouverez ci-dessous le ARN mappage de l'accord entre les ressources existantes et les ressources précises.

Nom de l'accord	Autorisations Artifact ARN for Legacy	Artifact ARN pour des autorisations précises
AWSAddendum relatif aux associés commerciaux	arn:aws:artifact : ::agreement/ Addendum relatif aux associés commerciaux AWS	arn:aws:artefact : ::accord/ agreement-9c1 T kBcYzn kcpRIm
AWSAddendum sur les violations de données à déclaration obligatoire en Nouvelle-Zélande	arn:aws:artifact : ::agreeme nt/ Addendum sur les violation s de données à déclarati on obligatoire en Nouvelle-Zélande AWS	arn:aws:artefact : ::accord/ accord-3 YRq9rGUIu72r7Gt
AWSAddendum sur les violations de données à déclaration obligatoire en Australie	arn:aws:artifact : ::agreeme nt/ Addendum australien sur les violations de données à déclaration AWS obligatoire	arn:aws:artefact : ::accord/ accord - 8 9 sbLSDe bitmAXNr
AWSSECRègle 17a-4 Addendum	arn:aws:artifact : ::agreeme nt/ Addendum à la règle 17a-4 AWS SEC	arn:aws:artefact : ::agreeme nt/agreement-bexgr7sjv XAW4Gxu
AWSSECRègle 18a-6 Addendum	arn:aws:artifact : ::agreeme nt/ Addendum à la règle 18a-6 AWS SEC	arn:aws:artefact : ::accord/ agreement- HZTdNwJuq OKLReXC
AWSAddenda « Organizations Business Associate »	arn:aws:artifact : ::agreeme nt/ Organizations Business Associate AWS Addendum	arn:aws:artefact : ::agreeme nt/agreement-y03 aUw MAEorHtqjv
AWSAddendum relatif aux violations de données à déclaration obligatoire en Australie pour les organisat ions	arn:aws:artifact : AWS ::agreement/ Organizat ions Australian Notificable Data Breach Addendum	arn:aws:artefact : ::Agreeme nt/Agreement-Y pDMFXTe PE7kEg4b
AWSOrganisations | Nouvelle Zélande | Addendum sur	arn:aws:artifact : ::agreeme nt/ Addendum sur les violation	arn:aws:artefact : ::accord/ accord - 3 V52 uojEjr vOnvrh

Nom de l'accord	Autorisations Artifact ARN for Legacy	Artifact ARN pour des autorisations précises
les violations de données à déclaration obligatoire	s de données à déclaration obligatoire en AWS Nouvelle-Zélande	

Exemples IAM de politiques pour AWS Artifact

Vous pouvez créer des politiques d'autorisation qui accordent des autorisations aux IAM utilisateurs. Vous pouvez accorder aux utilisateurs l'accès aux AWS Artifact rapports et la possibilité d'accepter et de télécharger des accords au nom d'un seul compte ou d'une organisation.

Les exemples de politiques suivants indiquent les autorisations que vous pouvez attribuer aux IAM utilisateurs en fonction du niveau d'accès dont ils ont besoin.

- Exemples de politiques pour gérer les AWS rapports avec des autorisations détaillées
- Exemples de politiques pour gérer les rapports tiers
- Exemples de politiques pour gérer les accords
- Exemples de politiques à intégrer AWS Organizations
- Exemples de politiques pour gérer les accords relatifs au compte de gestion
- Exemples de politiques pour gérer les accords organisationnels
- Exemples de politiques pour gérer les notifications

Example Exemples de politiques pour gérer les AWS rapports par le biais d'autorisations détaillées

> **Tip**
>
> Vous devriez envisager d'utiliser la stratégie AWSArtifactReportsReadOnlyAccess gérée au lieu de définir votre propre stratégie.

La politique suivante autorise le téléchargement de tous les AWS rapports par le biais d'autorisations détaillées.

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

La politique suivante accorde l'autorisation de télécharger uniquement les ISO rapports AWS SOCPCI, et par le biais d'autorisations détaillées.

```
{
  "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 Exemples de politiques pour gérer les rapports tiers

> **Tip**
>
> Vous devriez envisager d'utiliser la stratégie AWSArtifactReportsReadOnlyAccess gérée au lieu de définir votre propre stratégie.

Les rapports tiers sont désignés par la IAM ressource`report`.

La politique suivante autorise toutes les fonctionnalités des rapports tiers.

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

La politique suivante autorise le téléchargement de rapports tiers.

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

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

La politique suivante autorise la liste des rapports tiers.

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

La politique suivante autorise l'accès aux détails d'un rapport tiers pour toutes les versions.

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

La politique suivante autorise l'accès aux détails d'un rapport tiers pour une version spécifique.

```
{
```

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

> **Tip**
>
> Vous devriez envisager d'utiliser la politique AWSArtifactAgreementsFullAccess gérée AWSArtifactAgreementsReadOnlyAccess ou gérée au lieu de définir votre propre stratégie.

Example Exemples de politiques pour gérer les accords

La politique suivante autorise le téléchargement de tous les accords.

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

La politique suivante autorise l'acceptation de tous les accords.

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

La politique suivante autorise la résiliation de tous les accords.

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

La politique suivante accorde des autorisations pour consulter et exécuter les accords au niveau du compte.

```
{
  "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 Exemples de politiques à intégrer AWS Organizations

La politique suivante autorise la création du IAM rôle AWS Artifact utilisé pour s'intégrer à AWS Organizations. Le compte de gestion de votre organisation doit disposer de ces autorisations pour démarrer avec les accords organisationnels.

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

La politique suivante accorde l'autorisation d'accorder AWS Artifact les autorisations d'utilisation AWS Organizations. Le compte de gestion de votre organisation doit disposer de ces autorisations pour démarrer avec les accords organisationnels.

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

Example Exemples de politiques pour gérer les accords relatifs au compte de gestion

La politique suivante accorde des autorisations pour gérer les accords pour le compte de gestion.

```
{
  "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 Exemples de politiques pour gérer les accords organisationnels

La politique suivante accorde des autorisations pour gérer les accords organisationnels. Un autre utilisateur disposant des autorisations requises doit configurer les accords organisationnels.

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

La politique suivante accorde des autorisations pour consulter les accords organisationnels.

```
{
  "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 Exemples de politiques pour gérer les notifications

La politique suivante accorde des autorisations complètes pour utiliser AWS Artifact les notifications.

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

La politique suivante autorise la liste de toutes les configurations.

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

La politique suivante autorise la création d'une configuration.

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

La politique suivante autorise la modification d'une configuration.

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

```
      ]
    }
  ]
}
```

La politique suivante autorise la suppression d'une configuration.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La politique suivante autorise l'affichage des détails d'une configuration.

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

```
}
```

La politique suivante autorise l'enregistrement ou le désenregistrement des hubs de notification.

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

Utilisation de politiques AWS gérées pour AWS Artifact

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou que de nouvelles API opérations sont disponibles pour les services existants.

Pour plus d'informations, consultez la rubrique AWS Politiques gérées dans le IAMGuide de l'utilisateur.

AWS politique gérée : AWSArtifactReportsReadOnlyAccess

Vous pouvez attacher la politique `AWSArtifactReportsReadOnlyAccess` à vos identités IAM.

Cette politique accorde des *`read-only`* autorisations permettant de répertorier, de consulter et de télécharger des rapports.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `artifact`— Permet aux principaux de répertorier, de consulter et de télécharger des rapports depuis AWS Artifact.

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

AWS politique gérée : AWSArtifactAgreementsReadOnlyAccess

Vous pouvez attacher la politique `AWSArtifactAgreementsReadOnlyAccess` à vos identités IAM.

Cette politique autorise *read-only* l'accès à la liste des contrats de service AWS Artifact et au téléchargement des accords acceptés. Il inclut également les autorisations permettant de répertorier et de décrire les détails de l'organisation. En outre, la politique permet de vérifier si le rôle lié au service requis existe.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `artifact`— Permet aux principaux de répertorier tous les accords et de consulter les accords acceptés à partir de AWS Artifact.
- `IAM`— Permet aux principaux de vérifier si le rôle lié au service existe en utilisant GetRole.
- `organization`— Permet aux directeurs de décrire l'organisation et de répertorier les accès aux services pour l'organisation.

```
{
  "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 politique gérée : AWSArtifactAgreementsFullAccess

Vous pouvez attacher la politique `AWSArtifactAgreementsFullAccess` à vos identités IAM.

Cette politique accorde des *`full`* autorisations pour répertorier, télécharger, accepter et résilier les accords AWS Artifact. Il inclut également des autorisations permettant de répertorier et d'autoriser AWS l'accès aux services dans le service Organisation, ainsi que de décrire les détails de l'organisation. En outre, la politique permet de vérifier si le rôle lié au service requis existe et d'en créer un dans le cas contraire.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `artifact`— Permet aux mandants de répertorier, de télécharger, d'accepter et de AWS Artifact résilier les accords.
- `IAM`— Permet aux principaux de créer un rôle lié au service et de vérifier si le rôle lié au service existe en utilisant GetRole.
- `organization`— Permet aux responsables de décrire l'organisation et de lister/activer l'accès aux services pour l'organisation.

```
{
  "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 Artifact mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Artifact depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS fil sur la page Historique du AWS Artifact document.

Modification	Description	Date
AWS Artifact a commencé à suivre les modifications	AWS Artifact a commencé à suivre les modifications apportées AWS à ses politiques gérées et a introduit AWSArtifactReportsReadOnlyAccess.	15/12/2023

Modification	Description	Date
AWSContrats introduits, politiques gérées	Politiques introduites AWSArtifactAgreements ReadOnlyAccess et AWSArtifactAgreementsFullAccess gérées.	21/11/2024

Utilisation des rôles liés aux services pour AWS Artifact

AWS Artifact utilise AWS Identity and Access Management (IAM) des rôles liés à un service. Un rôle lié à un service est un type unique de IAM rôle directement lié à. AWS Artifact Les rôles liés au service sont prédéfinis par AWS Artifact et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Artifact car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Artifact définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Artifact peut assumer ses rôles. Les autorisations définies incluent la politique de confiance et la politique d'autorisations, et cette politique d'autorisations ne peut être attachée à aucune autre IAM entité.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Artifact ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôles liés à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Artifact

AWS Artifact utilise le rôle lié au service nommé AWSServiceRoleForArtifact— Permet de AWS Artifact recueillir des informations sur une organisation via. AWS Organizations

Le rôle AWSServiceRoleForArtifact lié à un service fait confiance aux services suivants pour assumer le rôle :

- `artifact.amazonaws.com`

La politique d'autorisations de rôle nommée AWSArtifactServiceRolePolicy AWS Artifact permet d'effectuer les actions suivantes sur la `organizations` ressource.

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

Création d'un rôle lié à un service pour AWS Artifact

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous accédez à l'onglet Accords d'organisation d'un compte de gestion d'organisation et que vous cliquez sur le lien Commencer dans le AWS Management Console, vous AWS Artifact créez le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous accédez à l'onglet Accords d'organisation d'un compte de gestion d'organisation et que vous cliquez sur le lien Commencer, le rôle lié au service est à nouveau AWS Artifact créé pour vous.

Modification d'un rôle lié à un service pour AWS Artifact

AWS Artifact ne vous permet pas de modifier le rôle AWSServiceRoleForArtifact lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Vous pouvez toutefois modifier la description du rôle à l'aide deIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Supprimer un rôle lié à un service pour AWS Artifact

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le AWS Artifact service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS Artifact les ressources utilisées par AWSServiceRoleForArtifact

1. Consultez le tableau « Accords d'organisation » dans la console AWS Artifact
2. Résilier tous les accords d'organisation en cours

Pour supprimer manuellement le rôle lié à un service à l'aide de IAM

Utilisez la IAM console AWS CLI, le ou le AWS API pour supprimer le rôle AWSServiceRoleForArtifact lié au service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Régions prises en charge pour les rôles AWS Artifact liés à un service

AWS Artifact ne prend pas en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Vous pouvez utiliser le AWSServiceRoleForArtifact rôle dans les régions suivantes.

Nom de la région	Identité de la région	Support dans AWS Artifact
US East (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Non
USA Ouest (Californie du Nord)	us-west-1	Non
USA Ouest (Oregon)	us-west-2	Oui
Afrique (Le Cap)	af-south-1	Non
Asie-Pacifique (Hong Kong)	ap-east-1	Non
Asie-Pacifique (Jakarta)	ap-southeast-3	Non

Nom de la région	Identité de la région	Support dans AWS Artifact
Asie-Pacifique (Mumbai)	ap-south-1	Non
Asie-Pacifique (Osaka)	ap-northeast-3	Non
Asie-Pacifique (Séoul)	ap-northeast-2	Non
Asie-Pacifique (Singapour)	ap-southeast-1	Non
Asie-Pacifique (Sydney)	ap-southeast-2	Non
Asie-Pacifique (Tokyo)	ap-northeast-1	Non
Canada (Centre)	ca-central-1	Non
Europe (Francfort)	eu-central-1	Non
Europe (Irlande)	eu-west-1	Non
Europe (Londres)	eu-west-2	Non
Europe (Milan)	eu-south-1	Non
Europe (Paris)	eu-west-3	Non
Europe (Stockholm)	eu-north-1	Non
Moyen-Orient (Bahreïn)	me-south-1	Non
Moyen-Orient (UAE)	me-central-1	Non
Amérique du Sud (São Paulo)	sa-east-1	Non
AWS GovCloud (USA Est)	us-gov-east-1	Non
AWS GovCloud (US-Ouest)	us-gov-west-1	Non

Utilisation de clés de IAM condition pour les AWS Artifact rapports

Vous pouvez utiliser les clés de IAM condition pour fournir un accès détaillé aux rapports sur AWS Artifact, en fonction de catégories et de séries de rapports spécifiques.

Les exemples de politiques suivants indiquent les autorisations que vous pouvez attribuer aux IAM utilisateurs en fonction de catégories et de séries de rapports spécifiques.

Example Exemples de politiques pour gérer l'accès en lecture aux AWS rapports

AWS Artifact les rapports sont désignés par la IAM ressource,`report`.

La politique suivante autorise la lecture de tous les AWS Artifact rapports de `Certifications and Attestations` cette catégorie.

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

La politique suivante vous permet d'autoriser la lecture de tous les AWS Artifact rapports de la SOC série.

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

La politique suivante vous permet d'autoriser la lecture de tous les AWS Artifact rapports, à l'exception de ceux de la `Certifications and Attestations` catégorie.

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

Enregistrement AWS Artifact API des appels avec AWS CloudTrail

AWS Artifact est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Artifact. CloudTrail capture API les appels AWS Artifact sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS Artifact console et des appels de code vers les AWS Artifact API opérations. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour AWS Artifact. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS Artifact, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS Artifact informations dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS Artifact, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre région Compte AWS, y compris des événements pour AWS Artifact, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge

- Configuration des SNS notifications Amazon pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

AWS Artifact prend en charge la journalisation des actions suivantes sous forme d'événements dans les fichiers CloudTrail journaux :

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

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'CloudTrail userIdentityélément.

Comprendre les entrées du fichier AWS Artifact journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l' GetReportMetadata action.


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

Historique du document pour AWS Artifact

Le tableau suivant fournit un historique des AWS Artifact versions et des modifications associées apportées au guide de l' AWS Artifact utilisateur.

Modification	Description	Date
Autorisations précises pour l'exécution des accords AWSArtifactAgreements FullAccess et politiques gérées AWSArtifactAgreements ReadOnlyAccess	Accès détaillé activé pour l'exécution des AWS Artifact accords et lancement AWSArtifactAgreementsFullAccesset AWSArtifactAgreementsReadOnlyAccess AWS gestion des politiques.	21 novembre 2024
Accès aux rapports précis et politique gérée AWSArtifactReportReadOnlyAccess	Accès détaillé aux rapports activé, activation des clés de condition des AWS Artifact rapports et lancement d'une politique AWSArtifactReportsReadOnlyAccessgérée.	15 décembre 2023
AWS Artifact rôle lié au service	Ajout de la documentation sur les rôles liés au service et mise à jour des exemples de politiques AWS Artifact et AWS Organizations d'intégration.	26 septembre 2023
Notifications	A publié la documentation relative à la gestion des notifications et a apporté les mises à jour pertinentes à la AWS Artifact API référence, à la documentation de CloudTrail journalisation et à la page de	1er août 2023

	gestion des identités et des accès.	
Rapports de tiers - Généralement disponibles	Ajout API de documentation de référence et de documentation de CloudTrail journalisation, et mise à disposition générale des rapports tiers.	27 janvier 2023
Rapports tiers (version préliminaire)	A publié des rapports de conformité des fournisseurs de logiciels indépendants (ISVs) qui vendent leurs produits sur AWS Marketplace. Des exemples de politiques ont été ajoutés à la page de gestion des identités et des accès pour les rapports tiers.	30 novembre 2022
Sécurité	Ajout d'une section à la page de gestion des identités et des accès pour éviter la confusion chez les adjoints.	20 décembre 2021
Rapports	Suppression de l'accord de confidentialité et introduction de termes et conditions pour le téléchargement des rapports.	17 décembre 2020
Page d'accueil et recherche	Ajout de la page d'accueil du service et de la barre de recherche sur la page des rapports et des accords.	15 mai 2020
GovCloud lancement	Lancé AWS Artifact en AWS GovCloud (US) Regions.	7 novembre 2019

AWS Organizations accords	Ajout de la prise en charge de la gestion des accords pour une organisation.	le 20 juin 2018
Accords	Support supplémentaire pour la gestion des AWS Artifact accords.	17 juin 2017
Première version	Cette version présente AWS Artifact.	30 novembre 2016

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.