Guide de l’utilisateur

AWS Artifact

AWS Artifact: Guide de l’utilisateur

Table of Contents

Qu'est-ce que AWS Artifact ?

AWS Artifactpropose des téléchargements à la demande de documents deAWS sécurité et de conformité, tels que les certificationsAWS ISO, les rapports PCI (Payment Card Industry) et les rapports SOC (Service Organization Control). Vous pouvez envoyer les documents relatifs à la sécurité et à la conformité (également connus sous le nom d'artefacts d'audit) à vos auditeurs ou régulateurs pour prouver la sécurité et la conformité de l'infrastructure et des services AWS que vous utilisez. Vous pouvez également utiliser ces documents comme lignes directrices pour évaluer votre propre architecture cloud et évaluer l'efficacité des contrôles internes de votre entreprise.

En outre,AWS Artifact vous pouvez télécharger à la demande des documents de sécurité et de conformité tels que les certifications ISO et les rapports de contrôle de l'organisation des services (SOC) des éditeurs de logiciels indépendants (ISV) qui vendent leurs produitsAWS Marketplace. Pour de plus amples informations, veuillez consulter Informations sur les AWS Marketplacefournisseurs Insights.

Les clients AWS sont responsables de l'élaboration ou de l'obtention des documents prouvant la sécurité et la conformité de leurs entreprises. Pour plus d'informations, consultez Modèle de responsabilité partagée.

Vous pouvez également utiliser AWS Artifact pour revoir, accepter et suivre l'état des accords AWS comme le Business Associate Addendum (BAA). Un BAA est généralement requis pour les entreprises soumises à la Health Insurance Portability and Accountability Act (HIPAA) pour s'assurer que les données de santé protégées (PHI) sont sécurisées comme il se doit. Avec AWS Artifact, vous pouvez accepter des accords avec AWS et désigner des comptes AWS autorisés à traiter légalement les informations à accès limité. Vous pouvez accepter un accord pour plusieurs comptes. Pour accepter des accords pour plusieurs comptes, utilisez AWS Organizations pour créer une organisation.

Pour plus d'informations, veuillez consulter AWS Artifact.

Tarification

AWSvous fournit gratuitement desAWS Artifact documents et des accords.

Démarrer avec AWS Artifact

AWS Artifactfournit une ressource centrale pour les rapports AWS de sécurité et de conformité. Les artefacts disponibles AWS Artifact incluent les rapports SOC (Service Organization Control), les rapports PCI (Payment Card Industry) et les certifications des organismes d'accréditation qui valident la mise en œuvre et l'efficacité opérationnelle des contrôles de AWS sécurité. AWS ArtifactFournit également un accès à la demande aux documents de sécurité et de conformité tels que les certifications ISO et les rapports SOC (Service Organization Control) des fournisseurs de logiciels indépendants (ISV) sur AWS Marketplace lesquels ils vendent leurs produits. Pour plus d'informations, consultez AWS MarketplaceVendor Insights.

AWS Artifactvous permet d'accepter et de gérer des accords juridiques tels que le Business Associate Addendum (BAA). Si vous utilisez AWS Organizations, vous pouvez accepter des accords pour tous les comptes de votre organisation. Une fois l'accord accepté, tous les comptes membres existants et suivants sont automatiquement couverts par cet accord.

Tâches

- Étape 1 : S'inscrire à AWS
- Étape 2 : Téléchargez un rapport
- Étape 3 : Gérer les accords
- Étape 4 : Gérer les notifications

Étape 1 : S'inscrire à AWS

Si vous n'avez pas de compte Compte AWS, procédez comme suit pour en créer un.

Pour s'inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous souscrivez à un Compte AWS, un Utilisateur racine d'un compte AWS est créé. Par défaut, seul l'utilisateur root a accès à l'ensemble des Services AWS et des ressources de

ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur administratif, et à uniquement utiliser l'utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

Étape 2 : Téléchargez un rapport

Vous pouvez télécharger des rapports à l'aide d'Adobe Acrobat Reader. Les autres lecteurs PDF ne sont pas pris en charge. Pour plus d'informations, consultez Téléchargement de rapports.

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 Artifactaccueil, choisissez Afficher les rapports.
3. Sur la page Rapports, utilisez l'onglet AWSRapports pour accéder à un AWS rapport et accédez à l'onglet Rapports tiers pour accéder aux rapports des fournisseurs de logiciels indépendants (ISV) sur AWS Marketplace lesquels ils vendent leurs produits.
4. (Facultatif) Entrez un mot clé dans le champ de recherche pour trouver un rapport.
5. Sélectionnez un rapport, puis choisissez Télécharger le rapport.
6. (Facultatif) Dans l'onglet Rapports tiers, vous pouvez accéder à la page de détails d'un rapport ISV en cliquant sur le titre du rapport pour en savoir plus sur le rapport.
7. Il peut vous être demandé d'accepter les conditions générales qui s'appliquent au rapport spécifique que vous êtes en train de télécharger. Nous vous recommandons de les lire attentivement. Lorsque vous avez terminé, sélectionnez J'ai lu et j'accepte les conditions, puis choisissez Accepter les conditions et télécharger le rapport.
8. Ouvrez le fichier téléchargé via une visionneuse PDF. 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 document PDF. Assurez-vous donc de vérifier la présence de pièces jointes dans le fichier PDF pour les pièces justificatives. Cliquez ici pour obtenir des instructions sur la façon d'afficher les pièces jointes.

Les rapports tiers ne sont accessibles qu'aux AWS clients qui ont intégré AWS Marketplace Vendor Insights. Pour en savoir plus, consultez AWS MarketplaceVendor Insights.

Étape 3 : Gérer les accords

Avant de conclure un accord, vous devez télécharger et accepter les termes de l'accord de AWS Artifact confidentialité (NDA). Chaque accord est confidentiel et ne peut pas être partagé avec d'autres personnes extérieures à votre entreprise.

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 de navigation AWS Artifact, choisissez Agreements (Accords).
3. Choisissez Accords de compte pour gérer les accords relatifs à votre compte ou Contrats d'organisation pour gérer les accords au nom de votre organisation.
4. Développez la section de l'accord.
5. Choisissez Télécharger et vérifier.
6. Lisez les termes et conditions. Lorsque vous avez terminé, choisissez Accepter et télécharger.
7. Passez en revue le contrat, puis cochez les cases pour indiquer que vous êtes d'accord.
8. Choisissez Accepter pour accepter le contrat.

Pour plus d'informations, consultez Gestion des accords.

Étape 4 : Gérer les notifications

Vous pouvez vous abonner aux notifications concernant la disponibilité de nouveaux rapports et accords ou les mises à jour de rapports et d'accords existants. AWS Artifact utilise le service de notification utilisateur AWS pour envoyer des notifications. Les notifications sont envoyées aux adresses e-mail fournies par l'utilisateur lors de la configuration de la configuration des notifications.

Pour créer une configuration

1. Ouvrez la page des centres de notifications dans le service AWS User Notifications
2. Sélectionnez la ou les régions dans lesquelles vous souhaitez stocker vos ressources de notifications utilisateur AWS. Par défaut, les données de vos notifications utilisateur seront stockées dans l'est des États-Unis (Virginie du Nord) et répliquées dans les autres régions que vous sélectionnez. Consultez la documentation des centres de notification pour plus de détails.
3. Cliquez sur Créer une configuration.

4. Pour recevoir des notifications relatives aux accords, cochez la case « Mises à jour des accords AWS ».
5. Pour recevoir des notifications relatives aux rapports, cochez la case Mises à jour sur les rapports AWS. Pour ne recevoir des notifications que pour les rapports relevant de catégories et de séries spécifiques, cochez la case Un sous-ensemble de rapports et cochez la case correspondant aux catégories et séries qui vous intéressent.
6. Entrez un nom pour votre configuration.
7. Entrez une liste d'e-mails séparés par des virgules où les notifications doivent être envoyées.
8. (Facultatif) Pour attribuer une balise à la configuration des notifications, entrez les paires clé-valeur en développant la section Tags. Remarque : Une balise est une étiquette que vous pouvez attribuer à une ressource AWS. Chaque balise est composée d'une clé et d'une valeur facultative que vous pouvez définir. Les balises vous aident à gérer, rechercher et filtrer les ressources.
9. Cliquez sur Soumettre.
10. Un e-mail de vérification sera envoyé aux adresses e-mail fournies et les destinataires devront cliquer sur le lien Vérifier l'e-mail dans l'e-mail de vérification qui leur a été envoyé. Veuillez noter que seules les adresses e-mail vérifiées commenceront à recevoir des notifications.

Pour plus d'informations, consultez Gestion des notifications.

Téléchargement de rapports dans AWS Artifact

Vous pouvez télécharger des rapports à partir de la console AWS Artifact. 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 exigent 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 plus d'informations, consultez Gestion des identités et des accès dans AWS Artifact.

Lorsque vous vous inscrivez à AWS Artifact, votre compte bénéficie automatiquement des autorisations de téléchargement de certains rapports. Si vous rencontrez des difficultés pour y accéderAWS 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 Artifactaccueil, choisissez Afficher les rapports.
3. Sur la page Rapports, utilisez l'onglet AWSRapports pour accéder à un AWS rapport et accédez à l'onglet Rapports tiers pour accéder aux rapports des fournisseurs de logiciels indépendants (ISV) sur AWS Marketplace lesquels ils vendent leurs produits.
4. (Facultatif) Entrez un mot clé dans le champ de recherche pour trouver un rapport.
5. Sélectionnez un rapport, puis choisissez Télécharger le rapport.

6. (Facultatif) Dans l'onglet Rapports tiers, vous pouvez accéder à la page de détails d'un rapport ISV en cliquant sur le titre du rapport pour en savoir plus sur le rapport.
7. Il peut vous être demandé d'accepter les conditions générales qui s'appliquent au rapport spécifique que vous êtes en train de télécharger. Nous vous recommandons de les lire attentivement. Lorsque vous avez terminé, sélectionnez J'ai lu et j'accepte les conditions, puis choisissez Accepter les conditions et télécharger le rapport.
8. Ouvrez le fichier téléchargé via un lecteur PDF. 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 document PDF. Assurez-vous donc de vérifier la présence de pièces jointes dans le fichier PDF pour les pièces justificatives. Cliquez ici pour obtenir des instructions sur la façon d'afficher les pièces jointes.

Affichage des pièces jointes dans des documents PDF

Les applications suivantes qui prennent actuellement en charge l'affichage des pièces jointes au format PDF sont recommandées :

Visionneuse Adobe Acrobat

1. Téléchargez la dernière version d'Adobe Acrobat ici.
2. Ouvrez le fichier dans Adobe Acrobat Viewer.
3. Pour ouvrir le panneau Pièces jointes, cliquez sur l'icône en forme de trombone à gauche du document PDF ou choisissez Affichage > Afficher/Masquer > Volets de navigation > Pièces jointes.
4. Dans le panneau Pièces jointes, double-cliquez sur la pièce jointe pour afficher le document.

Navigateur Firefox

1. Téléchargez le navigateur Firefox ici
2. Ouvrez le fichier PDF dans le navigateur Firefox en utilisant l'option Ouvrir le fichier dans le menu Fichier.
3. Pour ouvrir les pièces jointes, cliquez sur l'icône Toggle dans la barre latérale en haut à gauche de l'écran.

Sécurisation de vos documents

AWS Artifactles documents sont confidentiels et doivent être conservés en lieu sûr en tout temps. AWS Artifactutilise 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 Artifactpeut 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 la AWS Artifact FAQ.

Gestion des accords dans AWS Artifact

Les accords AWS Artifact vous permettent d'utiliser AWS Management Console pour consulter, accepter et gérer des accords pour votre compte ou votre organisation. Par exemple, un accord BAA (Business Associate Addendum) est généralement requis pour les entreprises soumises à la loi Health Insurance Portability and Accountability Act (HIPAA) pour s'assurer que les données de santé protégées (PHI) sont sécurisées comme il se doit. Vous pouvez utiliser AWS Artifact pour accepter un accord comme l'accord BAA avec AWS et désigner un compte AWS autorisé à traiter légalement les données de santé protégées. Si vous utilisez AWS Organizations, vous pouvez accepter des accords comme l'accord BAA AWS pour tous les comptes de votre organisation. Tous les comptes membres existants et suivants sont couverts automatiquement par l'accord et peuvent traiter légalement les données de santé protégées.

Vous pouvez également utiliser AWS Artifact pour vérifier que votre compte ou organisation AWS a accepté un accord et consulter les conditions de celui-ci afin de comprendre vos obligations. Si votre compte ou votre organisation n'a plus besoin d'utiliser l'accord accepté, vous pouvez le résilier. AWS Artifact 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

Gestion d'un contrat pour un compte unique dans AWS Artifact

Vous pouvez accepter des accords uniquement pour votre compte, même si votre compte est un compte membre appartenant à une organisation dans AWS Organizations. Pour plus d'informations sur AWS Organizations, consultez le AWS OrganizationsGuide de l'utilisateur .

Acceptation d'un accord avec AWS

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 aux utilisateurs IAM et aux utilisateurs fédérés dotés de rôles 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, les utilisateurs IAM et fédérés doivent disposer des autorisations suivantes :

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

Pour plus d'informations, veuillez consulter Gestion des identité et des accès.

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 de navigation AWS Artifact, choisissez Agreements (Accords).
3. Choisissez l'onglet Account agreements (Accords de compte).
4. Développez la section de l'accord.
5. Choisissez Télécharger et vérifier.
6. Lisez les termes et conditions. Lorsque vous avez terminé, choisissez Accepter et télécharger.
7. Passez en revue le contrat, puis cochez les cases pour indiquer que vous êtes d'accord.
8. Choisissez Accepter pour accepter l'accord relatif à votre compte.

Résiliation d'un accord avec AWS

Si vous avez utilisé la console AWS Artifact pour accepter un accord, vous pouvez l'utiliser pour le résilier. Sinon, consultez Contrats hors ligne.

Autorisations nécessaires

Pour résilier un accord, les utilisateurs IAM et fédérés doivent disposer des autorisations suivantes :

```
artifact:TerminateAgreement
```

Pour plus d'informations, veuillez consulter Gestion des identité et des accès.

Pour résilier un accord en ligne avec AWS

1. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.

2. Dans le volet de navigation AWS Artifact, choisissez Agreements (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 Terminer. Lorsque vous êtes invité à confirmer, choisissez Terminate (Mettre fin).

Gérer un accord pour plusieurs comptes dans AWS Artifact

Si vous êtes le propriétaire du compte de gestion d'une AWS Organizations organisation, vous pouvez accepter un accord au nom de tous les comptes de votre organisation. Vous devez être connecté au compte de gestion avec les AWS Artifact autorisations appropriées pour accepter ou résilier les accords d'organisation. Les utilisateurs de comptes membres avec des autorisations `organizations:DescribeOrganization` peuvent consulter les accords d'organisation qui sont acceptés en leur nom.

Si votre compte ne fait pas partie d'une organisation, vous pouvez créer ou rejoindre une organisation en suivant les instructions de la section Création et gestion d'une organisation du Guide de l'AWS Organizationsutilisateur.

Deux ensembles de fonctions sont disponibles pour AWS Organizations : fonctions de facturation consolidée et toutes les fonctions. Pour utiliser AWS Artifact pour votre organisation, l'organisation à laquelle vous appartenez doit être activée pour toutes les fonctions. 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.

Si un compte membre est supprimé d'une organisation, ce compte n'est plus couvert par les accords d'organisation. Les administrateurs de compte de gestion doivent communiquer cette suppression aux comptes membres avant de supprimer les comptes membres de l'organisation, afin que les comptes membres puissent mettre en place de nouveaux accords, si nécessaire. La liste des accords d'organisation actifs peut être consultée dans Accords d'AWS Artifactorganisation.

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

Acceptation d'un accord pour votre organisation

Vous pouvez accepter un accord pour tous les comptes membres de votre organisation dans AWS Organizations. Avant d'accepter un accord, nous vous recommandons de consulter votre équipe en charge des aspects juridiques, de confidentialité et de conformité.

Autorisations nécessaires

Pour accepter un accord, le propriétaire du compte de gestion doit disposer des autorisations suivantes :

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

Pour plus d'informations, veuillez consulter Gestion des identité et des accès.

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 tableau de bord AWS Artifact, choisissez Agreements (Accords).
3. Choisissez l'onglet Organization agreements (Accords d'organisation).
4. Développez la section de l'accord.
5. Choisissez Télécharger et vérifier.
6. Lisez les termes et conditions. Lorsque vous avez terminé, choisissez Accepter et télécharger.
7. Passez en revue le contrat, puis cochez les cases pour indiquer que vous êtes d'accord.
8. Choisissez Accept (Accepter) pour accepter l'accord pour tous les comptes existants et futurs de votre organisation.

Résiliation d'un accord d'organisation

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

Autorisations nécessaires

Pour résilier un accord, le propriétaire du compte de gestion doit disposer des autorisations suivantes :

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

Pour plus d'informations, veuillez consulter Gestion des identité et des accès.

Pour résilier un accord d'organisation en ligne avec AWS

1. Ouvrez la AWS Artifact console à l'adresse https://console.aws.amazon.com/artifact/.
2. Sur le tableau de bord AWS Artifact, choisissez Agreements (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 Terminer. Lorsque vous êtes invité à confirmer, choisissez Terminate (Mettre fin).

Gestion d'un accord hors ligne existant dans AWS Artifact

Si vous disposez d'un accord hors ligne existant, AWS Artifact affiche les accords que vous avez acceptés hors ligne. Par exemple, la console peut afficher Offline Business Associate Addendum (BAA) avec l'état Active (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 suivantes :

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

Si votre compte est un compte membre d'une organisation, vous devez disposer des autorisations suivantes pour afficher vos accords d'organisation hors ligne :

```
organizations:DescribeOrganization
```

Pour plus d'informations, veuillez consulter Gestion des identité et des accès.

Gestion des notifications dans AWS Artifact

Les notifications AWS Artifact vous permettent de configurer des notifications par e-mail. Sur la page des paramètres de notification, vous pouvez vous abonner aux notifications et gérer les autres paramètres de notification comme décrit ci-dessous. AWS Artifact envoie des notifications à l'aide du service AWS User Notifications. Pour utiliser les notifications AWS Artifact, vous devez disposer des autorisations requises pour les services AWS Artifact et AWS User Notification. Pour plus d'informations, veuillez consulter Gestion des identité et des accès.

Table des matières

Configuration de vos notifications

Avant de commencer à recevoir des notifications, vous devez spécifier la ou les régions dans lesquelles les données de vos notifications utilisateur seront stockées. Suivez les étapes ci-dessous pour configurer les hubs de notification.

Pour configurer les hubs de notifications

1. Ouvrez la page des centres de notifications dans le service AWS User Notifications.
2. Sélectionnez la ou les régions dans lesquelles vous souhaitez stocker vos ressources de notifications utilisateur AWS. Par défaut, les données de vos notifications utilisateur seront stockées dans l'est des États-Unis (Virginie du Nord) et seront répliquées dans les autres régions que vous avez sélectionnées. Reportez-vous à la documentation des centres de notification pour plus de détails.
3. Cliquez sur Soumettre.

Pour s'abonner aux notifications

1. Ouvrez la page des paramètres de notification d'AWS Artifact.
2. Cliquez sur le bouton S'abonner aux notifications Artifact pour vous abonner aux notifications sur AWS Artifact.

Pour vous désabonner des notifications

1. Ouvrez la page des paramètres de notification d'AWS Artifact.
2. Cliquez sur le bouton S'abonner aux notifications Artifact pour vous désabonner des notifications sur AWS Artitfact.

Pour créer une configuration

1. Ouvrez la page des paramètres de notification d'AWS Artifact.
2. Cliquez sur Créer une configuration.
3. Pour recevoir des notifications relatives aux accords, maintenez la case à cocher cochée à côté de Mises à jour des accords AWS.
4. Pour recevoir des notifications relatives aux rapports, maintenez la case à cocher cochée à côté de Mises à jour des rapports AWS.
5. Pour recevoir des notifications pour tous les rapports, maintenez la case cochée à côté de Tous les rapports.
6. Pour recevoir des notifications uniquement pour les rapports relevant de catégories et de séries spécifiques, cochez la case Un sous-ensemble de rapports. Cliquez ensuite sur la case correspondant aux catégories et séries qui vous intéressent.
7. Entrez un nom pour votre configuration.
8. Entrez une liste d'e-mails séparés par des virgules où les notifications doivent être envoyées.
9. (Facultatif) Pour attribuer une balise à la configuration des notifications, entrez les paires clé-valeur en développant la section Tags. Remarque : Une balise est une étiquette que vous pouvez attribuer à une ressource AWS. Chaque balise est composée d'une clé et d'une valeur facultative que vous pouvez définir. Les balises vous aident à gérer, rechercher et filtrer les ressources.
10. Cliquez sur Créer une configuration.
11. Un e-mail de vérification sera envoyé aux adresses e-mail fournies et les destinataires devront cliquer sur le lien Vérifier l'e-mail dans l'e-mail de vérification qui leur a été envoyé. Veuillez noter que seules les adresses e-mail vérifiées commenceront à recevoir des notifications.

Pour modifier une configuration

1. Ouvrez la page des paramètres de notification d'AWS Artifact.

2. Cliquez sur la ligne de la configuration que vous souhaitez modifier.
3. Cliquez sur le bouton Modifier en haut à droite de la page.
4. Vous pouvez modifier n'importe quel champ. Une fois que vous êtes satisfait de votre modification, appuyez sur Enregistrer les modifications.
5. Si vous avez ajouté de nouvelles adresses e-mail, un e-mail de vérification sera envoyé à chacune de ces adresses e-mail. Cliquez sur le lien Vérifier l'e-mail contenu dans l'e-mail de vérification.

Pour supprimer une configuration

1. Ouvrez la page des paramètres de notification d'AWS Artifact.
2. Cliquez sur la ligne de la configuration que vous souhaitez supprimer.
3. Cliquez sur Delete.
4. Après avoir lu le message d'avertissement, cliquez sur Supprimer.

Affectation de balises à une configuration

Une balise est une étiquette que vous affectez à une ressource AWS. Chaque étiquette est constituée d'une clé et d'une valeur facultative que vous définissez. Les balises vous aident à gérer, rechercher et filtrer les ressources. Vous pouvez éventuellement définir des balises lorsque vous créez ou modifiez une configuration. Pour en savoir plus, consultez la section Ressources de balisage

Résolution des problèmes

Si vous recevez un message d'erreur lors de l'utilisation des notifications AWS Artifact, consultez la section Résolution des problèmes dans la AWS Artifact FAQ.

Gestion des identités et des accès dans AWS Artifact

Lorsque vous vous inscrivez à AWS, vous fournissez une adresse e-mail et un mot de passe qui sont associés à votre compte AWS. Il s'agit de vos informations d'identification root, qui fournissent un accès complet à toutes vos AWS ressources, y compris aux ressources pourAWS 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 utilisateur IAM pour vous-même et pour toute personne susceptible d'avoir besoin d'accéder à un document ou à AWS Artifact un accord. 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 les autorisations à un groupe IAM et en ajoutant les utilisateurs IAM au groupe.

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

Table des matières

Configurer l'accès des utilisateurs 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 politique IAM

En tant qu'administrateur IAM, 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 politique IAM que vous pouvez utiliser pour accorder des autorisations à vos utilisateurs et groupes IAM.

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Policies (Politiques).
3. Sélectionnez Create policy (Créer une politique).
4. Choisissez l'onglet JSON.
5. Entrez un document de politique. Vous pouvez créer votre propre politique ou utiliser l'une des politiques deExemple de politiques IAM.
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 groupe IAM et associer la politique

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

Pour créer un groupe IAM 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 utilisateurs IAM et les ajouter au groupe

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

Pour créer un utilisateur IAM 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 à AWS 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 vers des autorisations détaillées

AWS Artifact permet désormais aux clients d'utiliser des autorisations détaillées. Grâce à ces autorisations détaillées, les clients auront un contrôle précis sur l'accès à des fonctionnalités telles que l'acceptation des conditions et le téléchargement de rapports.

Pour accéder aux rapports via les autorisations détaillées, les clients doivent utiliser la politique AWSArtifactReportsReadOnlyAccess gérée ou mettre à jour leurs autorisations conformément à la recommandation ci-dessous. Les clients doivent ensuite s'inscrire en cliquant sur le lien « Essayer la nouvelle page de rapports AWS » disponible dans la console.

Les utilisateurs auront la possibilité d'accéder aux rapports avec les anciennes autorisations en utilisant le lien de la page des anciens rapports disponible dans la console en cas de problème lors de la mise à jour des nouvelles autorisations.

Migration vers de nouvelles autorisations

Migrer les autorisations non spécifiques aux ressources

Les utilisateurs doivent remplacer la politique existante contenant les anciennes autorisations par une politique contenant des autorisations détaillées

Politique relative aux héritages :

```
{
  "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

Les utilisateurs doivent remplacer leur politique existante contenant des autorisations héritées par une politique contenant des autorisations détaillées. Les autorisations génériques des ressources du rapport ont été remplacées par des clés de condition.

Politique relative aux héritages :

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

Exemple de politiques IAM

Vous pouvez créer des politiques d'autorisation qui accordent des autorisations aux utilisateurs IAM. 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 utilisateurs IAM 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 autorise le téléchargement uniquement des rapports AWS SOC, PCI et ISO 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 ressource IAM. `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.

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

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

Example Exemples de politiques pour gérer les accords

La politique suivante autorise le téléchargement de tous les accords. Les utilisateurs IAM doivent également disposer de cette autorisation pour accepter des accords.

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

La politique suivante autorise l'acceptation d'un accord.

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

```
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La politique suivante autorise la résiliation d'un accord.

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

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

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

```
    }
  ]
}
```

Example Exemples de politiques à intégrer AWS Organizations

La politique suivante autorise la création du rôle IAM 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": [
    {
      "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"
    }
  ]
}
```

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": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
```

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

Example 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": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

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

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

```
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 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": [
        "*"
      ]
    }
  ]
}
```

AWSpolitiques gérées pour AWS Artifact

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS 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.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. 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 gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes

les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWSpolitique gérée : AWSArtifactReportsReadOnlyAccess

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

Cette politique accorde des autorisations de *`lecture seule`* qui permettent 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 depuisAWS Artifact.

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

Mises à jour d'Artifact apportées aux politiques gérées AWS

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour 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 fil RSS sur la page d'historique du document Artifact.

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

Utilisation de rôles liés à un service pour AWS Artifact

AWS Artifact utilise des rôles liés à un AWS Identity and Access Management service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à AWS Artifact. Les rôles liés à un 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 d'AWS Artifact, car il n'est pas nécessaire d'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 comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

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

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées à un service pour AWS Artifact

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

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

- `artifact.amazonaws.com`

La politique d'autorisation de rôle nommée AWSArtifactServiceRolePolicy permet à AWS Artifact 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 Organizations Agreements d'un compte de gestion d'organisation et que vous sélectionnez le lien « Get started » dans le compteAWS Management Console, AWS Artifact crée pour vous le rôle lié au service.

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 Organizations Agreements d'un compte de gestion d'organisation et que vous sélectionnez le lien « Commencer », AWS Artifact crée à nouveau le rôle lié au service pour vous.

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

AWS Artifact ne vous permet pas de modifier le rôle lié au AWSServiceRoleForArtifact 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. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'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 service AWS Artifact 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 les ressources AWS Artifact utilisées par AWSServiceRoleForArtifact

1. Consultez le tableau « Contrats 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 d'IAM

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

Régions prises en charge pour les rôles liés au service AWS Artifact

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

Nom de la région	Identité de la région	Support dans AWS Artifact
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
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 (EAU)	me-central-1	Non
Amérique du Sud (São Paulo)	sa-east-1	Non

Nom de la région	Identité de la région	Support dans AWS Artifact
AWS GovCloud (USA Est)	us-gov-east-1	Non
AWS GovCloud (US-Ouest)	us-gov-west-1	Non

Utilisation des clés de condition IAM

Vous pouvez utiliser les clés de condition IAM 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 utilisateurs IAM en fonction de catégories et de séries de rapports spécifiques.

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

AWS Artifactles rapports sont désignés par la ressource IAM,. `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"
        }
      }
    }
  ]
}
```

Journalisation des appels d'API AWS Artifact avec AWS CloudTrail

AWS Artifactest intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dansAWS Artifact. CloudTrail capture les appels d'API AWS Artifact sous forme d'événements. Les appels capturés incluent des appels de la console AWS Artifact et les appels de code vers les opérations d'API AWS Artifact. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pourAWS 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 faiteAWS 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 Artifactinformations dans CloudTrail

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

Pour un enregistrement continu des événements dans votre Compte AWS, y compris les événements pour AWS Artifact, créez un journal d'activité. 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 d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. 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 en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail

- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

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

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

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 effectuée avec les informations d'identification utilisateur racine 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 requête a été effectuée par un autre service AWS.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Présentation des AWS Artifact entrées des fichiers journaux

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 appels d'API 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 décrit toutes les versions des AWS Artifact.

Modification	Description	Date
Accès aux rapports précis et politique gérée AWSArtifactReportReadOnlyAccess	Accès détaillé aux rapports Artifact, activation des clés de condition des rapports et lancement d'une politique gérée. AWSArtifactReportsReadOnlyAccess	15 décembre 2023
Rôle lié au service AWS Artifact	Ajout de la documentation sur les rôles liés aux services et exemples de politiques mis à jour pour l'intégration d'AWS Artifact et d'AWS Organizations.	26 septembre 2023
Notifications	Publication de la documentation relative à la gestion des notifications et mise à jour pertinente du guide de référence des API, de la documentation de CloudTrail journalisation et de la page AWS Artifact Identity and Access Management.	1er août 2023
Rapports de tiers - Généralement disponibles	Ajout de la documentation de référence de l'API, de la documentation de CloudTrail journalisation et mise à disposition générale des rapports tiers.	27 janvier 2023

Rapports tiers (version préliminaire)	Lancement des rapports de conformité des fournisseurs de logiciels indépendants (ISV) qui vendent leurs produits surAWS Marketplace. En outre, 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 dans GovCloud les régions.	7 novembre 2019
AWS Organizationsaccords	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.