Guide de l’utilisateur

AWS Conducteur de facturation

AWS Conducteur de facturation: Guide de l’utilisateur

Table of Contents

Qu'est-ce que AWS Billing Conductor ?

AWS Billing Conductor est un service de facturation personnalisé destiné aux partenaires de AWS Marketplace distribution (partenaires) et aux organisations qui ont des exigences en matière de rétrofacturation. Pour les partenaires, les rétrofacturations sont une condition préalable pour être payés par leurs clients et respecter une Compte AWS limite AWS Organizations de facturation. Pour les organisations, les activités de rétrofacturation garantissent que les organisations affectent les coûts d'une équipe spécifique (par exemple, un ensemble de comptes) au budget interne ou au bon relevé de profits et pertes (P&L).

Pour réaliser ces activités, Billing Conductor permet aux clients de créer une deuxième version pro forma de leurs coûts à partager avec leurs clients ou les titulaires de comptes. Les coûts pro forma représentent l'utilisation au sein des comptes gérés par Billing Conductor (ceux affectés aux groupes de facturation) aux taux de tarification définis dans Billing Conductor (par exemple, en utilisant une règle de tarification globale pour appliquer une tarification publique à toutes les utilisations).

> **Note**
>
> Les clients constateront des différences d'utilisation mineures entre les coûts facturables (correspondant à la AWS facture) et les coûts pro forma (correspondant à la configuration de Billing Conductor) tout au long du mois. Toutefois, les valeurs d'utilisation seront identiques à la fin de chaque mois, une fois la AWS facture émise.

La définition des coûts pro forma permet aux clients de modéliser leurs coûts de manière uniforme pour qu'ils correspondent à l'un des cas d'utilisation suivants :

1. Les accords avec les clients, qui peuvent être un cas d'utilisation du partenaire, négociés en dehors de AWS
2. Pratiques comptables internes, souvent un cas d'utilisation spécifique à l'organisation

Les configurations de Billing Conductor n'affectent pas les factures AWS ou les configurations de facturation existantes des clients (par exemple, le partage de crédits ou les remises basées sur des engagements, comme les instances réservées ou les Savings Plans).

Les clients peuvent analyser les coûts pro forma à partir du compte de gestion en effectuant les tâches suivantes :

- Analysez les marges (la différence entre les coûts pro forma et les coûts facturables pour le même ensemble de comptes) dans Billing Conductor
- Consultez les coûts pro forma mensuels sur la page des détails de facturation
- Créez un AWS Cost and Usage Report (CUR) par groupe de facturation

Les comptes gérés par Billing Conductor (comptes appartenant à des groupes de facturation) peuvent analyser les coûts pro forma dans AWS Cost Explorer les rapports sur les coûts et l'utilisation, le tableau de bord de facturation et la page des détails de facturation.

Vous pouvez configurer les groupes de facturation, les plans tarifaires, les règles de tarification et les éléments de ligne personnalisés dans la console Billing Conductor ou à l'aide de l'API Billing Conductor.

Pour plus d'informations sur les quotas de service AWS de Billing Conductor, consultezQuotas et restrictions.

Rubriques

- Fonctionnalités de AWS Billing Conductor
- Services connexes

Fonctionnalités de AWS Billing Conductor

Vous pouvez utiliser les fonctionnalités AWS de Billing Conductor pour effectuer les opérations suivantes :

Comptes de groupe

Organisez les comptes en groupes de facturation pour obtenir une vue agrégée des coûts pro forma. Simulez des avantages individuels pour chaque client, tels que des remises multiservices, et Niveau gratuit d'AWS pour chaque groupe.

Tarification personnalisée

Définissez des majorations ou des remises globales ou spécifiques, et contrôlez l'accès au niveau gratuit.

Charges et crédits

Ajoutez des frais ou des crédits uniques ou récurrents forfaitaires ou basés sur un pourcentage aux groupes de facturation.

Analyse pro forma

Analysez les coûts en fonction des configurations de tarification dans la console de facturation. Les comptes de vos groupes de facturation peuvent visualiser, prévoir et créer des rapports personnalisés sur leurs coûts pro forma dans AWS Cost Explorer. Le compte principal aura une vue croisée de tous les coûts accumulés par les comptes du groupe de facturation, tandis que les comptes non principaux verront leurs propres coûts.

Génération de rapports

Configurez les rapports de coûts et d'utilisation pour chaque groupe de facturation.

Analyse des taux

Comparez les taux appliqués aux AWS taux réels avec le rapport sur les marges du groupe de facturation.

Services connexes

AWS Console de facturation

La console AWS de facturation est le portail destiné à tous les AWS clients, qu'il s'agisse d'étudiants, de jeunes entreprises ou de grandes entreprises. Vous pouvez utiliser la console pour voir les ressources qui s'exécutent sur vos AWS comptes, gérer les préférences de facturation et accéder aux artefacts de facturation nécessaires pour effectuer des paiements AWS. La console AWS de facturation fournit également une explication détaillée des dépenses de votre compte et sert de point d'entrée pour l'inscription aux produits des produits de gestion des AWS coûts.

Pour plus d’informations, consultez le Guide de l’utilisateur AWS Billing.

AWS Cost Explorer

Vous pouvez utiliser l'interface Cost Explorer pour visualiser, comprendre et gérer vos AWS coûts et votre utilisation au fil du temps. Commencez rapidement en créant des rapports personnalisés qui analysent les données relatives aux coûts et à l'utilisation. Analysez vos données à un niveau élevé (par exemple, les coûts totaux et l'utilisation pour tous les comptes), ou approfondissez vos données de coûts et d'utilisation pour identifier les tendances, identifier les facteurs de coûts et détecter les anomalies.

Pour plus d’informations, consultez les rubriques suivantes :

- Réalisation d'une analyse ad hoc sur les coûts pro forma dans AWS Cost Explorer

- Analysez vos coûts AWS Cost Explorer dans le guide de AWS Cost Management l'utilisateur

AWS Rapports de coûts et d'utilisation

Les rapports sur les AWS coûts et l'utilisation (AWS CUR) contiennent l'ensemble le plus complet de données sur les coûts et l'utilisation disponibles. Vous pouvez utiliser les rapports sur les coûts et l'utilisation pour publier vos rapports de AWS facturation dans un compartiment Amazon Simple Storage Service (Amazon S3) dont vous êtes le propriétaire. Vous pouvez recevoir des rapports qui détaillent vos coûts par heure ou par jour, par produit ou ressource de produit, ou par balises que vous définissez vous-même.

AWS met à jour le rapport de votre compartiment une fois par jour sous forme de valeurs séparées par des virgules (CSV) ou au format Apache Parquet. Vous pouvez consulter les rapports à l'aide d'un tableur tel que Microsoft Excel ou Apache OpenOffice Calc. Vous pouvez également y accéder depuis une application à l'aide des API Amazon S3 ou Amazon Athena.

AWS Les rapports sur les coûts et l'utilisation suivent votre AWS utilisation et fournissent une estimation des frais associés à votre compte. Chaque rapport contient des rubriques correspondant à chaque combinaison unique de AWS produits, de type d'utilisation et d'opération que vous utilisez dans votre AWS compte.

AWS Identity and Access Management (JE SUIS)

Le service AWS Billing Conductor est intégré à AWS Identity and Access Management (IAM). Vous pouvez utiliser IAM avec AWS Billing Conductor pour garantir que les autres personnes travaillant sur votre compte n'ont que l'accès dont elles ont besoin pour accomplir leur travail.

Vous utilisez également IAM pour contrôler l'accès à toutes vos AWS ressources. Cela inclut, mais sans s'y limiter, vos informations de facturation. Il est important que vous vous familiarisiez avec les concepts de base et les meilleures pratiques de l'IAM avant d'aller trop loin dans la configuration de la structure de votre AWS compte.

Pour plus d'informations sur la façon de travailler avec IAM, voir Qu'est-ce que l'IAM ? et les meilleures pratiques de sécurité en matière d'IAM dans le guide de l'utilisateur IAM.

AWS Organizations (Facturation consolidée)

AWS les produits et services peuvent convenir à toutes les tailles d'entreprises, des petites entreprises en démarrage aux entreprises. Si votre entreprise est de grande taille, ou susceptible de croître, vous pouvez configurer plusieurs comptes AWS afin de refléter la structure de votre entreprise. Par exemple, vous pouvez avoir un compte pour l'ensemble de l'entreprise et des comptes pour chaque employé, ou un compte pour l'ensemble de l'entreprise avec des utilisateurs

IAM pour chaque employé. Vous pouvez avoir un compte pour l'ensemble de l'entreprise, des comptes pour chaque service ou équipe au sein de l'entreprise et des comptes pour chaque employé.

Si vous créez plusieurs comptes, vous pouvez utiliser la fonction de facturation consolidée AWS Organizations pour regrouper tous vos comptes membres sous un seul compte de gestion et recevoir une facture unique. Pour plus d'informations, consultez la section Facturation consolidée pour les Organisations dans le Guide de AWS Billing l'utilisateur.

Comprendre votre tableau de bord AWS Billing Conductor

Le tableau de bord AWS Billing Conductor fournit un résumé de haut niveau des indicateurs clés pour vous aider à comprendre l'impact de vos dimensions de tarification personnalisées.

Indicateurs de performance clés

Cette section définit les indicateurs de performance clés (KPI) disponibles sur votre tableau de bord AWS Billing Conductor. Les KPI sont tousmonth-to-date. Au fur et à mesure que vous créez ou ajoutez des comptes à votre compteAWS Organizations, les comptes sont comptabilisés selon ce KPI. Lorsque vous supprimez un groupe de facturation, les comptes de ce groupe de facturation sont également associés à ce KPI.

- Montant facturé : frais d'utilisation combinés accumulés par tous les groupes de facturation, sur la base du tarif personnalisé défini par les plans tarifaires appliqués. Le calcul ne tient pas compte des remises basées sur des engagements achetées en dehors du groupe de facturation, des prix non publics ou des crédits consommés dans le domaine facturable. Les exemples de remises basées sur des engagements incluent les instances réservées et les plans d'épargne.
- AWScoûts : month-to-date frais d'utilisation combinés accumulés par tous les groupes de facturation, en fonction des frais estimés figurant sur votre AWS facture. Les calculs incluent toutes les remises basées sur des engagements achetées en dehors du groupe de facturation si ces avantages ont été appliqués au domaine facturable, tous les prix non publics, les remises échelonnées en fonction du volume et les crédits. Les exemples de remises basées sur des engagements incluent les instances réservées et les plans d'épargne.
- Marge : month-to-date marge agrégée accumulée par tous les groupes de facturation. La marge est calculée en soustrayant les AWS coûts du montant facturé. Sur la base de facteurs tels que le plan tarifaire et les rubriques personnalisées appliquées, la marge peut également être négative.

  > **Note**
  >
  > Les ajustements effectués après la période de facturation ont une incidence sur vos marges historiques. Pour plus d'informations, veuillez consulter Analyse de vos marges par groupe de facturation.

- Groupes de facturation : nombre de groupes de comptes mutuellement exclusifs, avec un compte principal et un plan tarifaire associé.

- Comptes surveillés : nombre de comptes d'une famille de facturation consolidée qui sont actuellement affectés à un groupe de facturation.
- Comptes non surveillés : nombre de comptes d'une famille de facturation consolidée qui n'ont pas été affectés à un groupe de facturation.

Autres définitions de AWS Billing Conductor

Cette section définit les autres termes utilisés dans AWS Billing Conductor pour vous aider à utiliser le service de manière efficace.

- Facturable : résultat de facturation généré par AWS et utilisé comme biais de calcul de votre AWS facture.
- Pro forma : sortie générée par AWS Billing Conductor. Cela correspond aux modifications que vous souhaitez apporter à la gestion des tarifs (configuration des prix) et à la visibilité agrégée des comptes (groupes de facturation).
- Valeurs des ressources : entrées utilisées pour calculer les éléments de ligne personnalisés basés sur des pourcentages. Les valeurs des ressources incluent les coûts accumulés pour le groupe de facturation et tous les éléments de ligne personnalisés fixes associés à un groupe de facturation donné pour une période de facturation.

Afficher vos cinq principaux groupes de facturation par montant facturé

Vous pouvez comprendre vos cinq principaux groupes de facturation qui génèrent des revenus en vous référant à la vue visuelle et à la vue tabulaire. Pour gérer vos groupes de facturation existants, choisissez Gérer les groupes de facturation sur la page du tableau de bord.

Création de groupes de facturation, de configurations de tarification et de rubriques personnalisées

Cette section explique comment créer des groupes de facturation, des configurations de tarification et des éléments de ligne personnalisés dans AWS Billing Conductor. Chaque section fournit également un aperçu de la manière dont vous pouvez utiliser le tableau des groupes de facturation, le tableau des règles de tarification et le tableau des articles personnalisés après avoir créé chaque article.

Rubriques

Création de groupes de facturation

Vous pouvez utiliser AWS Billing Conductor pour créer des groupes de facturation afin d'organiser vos comptes. Par défaut, les comptes payeurs dotés d'autorisations d'administrateur peuvent créer des groupes de facturation. Chaque groupe de facturation s'exclut mutuellement. Cela signifie qu'un compte ne peut appartenir qu'à un seul groupe de facturation au cours d'une période de facturation donnée. Bien que vous puissiez voir immédiatement la segmentation des groupes de facturation, il faut jusqu'à 24 heures après la création d'un groupe de facturation pour que les taux personnalisés du groupe soient reflétés.

> **Note**
>
> Le transfert de comptes entre groupes de facturation au milieu du mois initiera le recalcul des deux groupes de facturation jusqu'au début de la période de facturation. Le transfert de comptes en milieu de mois n'a aucune incidence sur les périodes de facturation précédentes.

Suivez les étapes ci-dessous pour créer un groupe de facturation.

Pour créer un groupe de facturation

1. Connectez-vous au AWS Management Console et ouvrez-le AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, choisissez Billing groups.
3. Choisissez Créer un groupe de facturation.
4. Pour les détails du groupe de facturation, entrez le nom du groupe de facturation. Pour les restrictions de dénomination, voirQuotas et restrictions.
5. (Facultatif) Dans Description, entrez une description pour le groupe de facturation.
6. Pour Plan tarifaire, choisissez un plan tarifaire à associer au groupe de facturation. Pour créer un plan tarifaire, voirCréation de plans de tarification.
7. (Facultatif) Pour les paramètres supplémentaires, vous pouvez activer l'association automatique de comptes pour le groupe de facturation.

   > Remarques
   >
   > - Un seul groupe de facturation peut être associé automatiquement à un compte.
   > - Une fois cette fonctionnalité activée, les comptes créés ou ajoutés à votre organisation seront automatiquement associés à ce groupe de facturation.
   > - Si vous disposez actuellement d'une trace de CloudTrail journalisation, vous pouvez consulter les associations automatiques de vos comptes dans votre CloudTrail journal.

8. Sous Comptes, choisissez un ou plusieurs comptes à ajouter au groupe de facturation ou choisissez Importer une unité organisationnelle pour sélectionner automatiquement les comptes appartenant à une unité organisationnelle. Pour un exemple de politique permettant d'accorder l'accès à la fonctionnalité d'importation de l'unité d'organisation, voirAccorder à Billing Conductor l'accès à la fonctionnalité d'importation d'unités organisationnelles.

   Vous pouvez utiliser le filtre de tableau pour trier par nom de compte, ID de compte ou adresse e-mail racine associée à un compte.
9. Le compte principal hérite de la possibilité de consulter les coûts et l'utilisation pro forma dans l'ensemble du groupe de facturation et peut générer des rapports de coûts et d'utilisation (AWS CUR) pro forma pour le groupe de facturation.

   Si vous choisissez un compte principal qui a rejoint votre organisation au cours du mois en cours, les coûts pro forma pour tous les comptes de ce groupe de facturation incluront

uniquement les coûts et l'utilisation accumulés depuis que le compte principal a rejoint l'organisation. Pour vérifier la date d'adhésion, choisissez Valider la date d'adhésion. Pour plus d'informations, consultez Comprendre l'importance de la date d'adhésion au compte principal.

10. Choisissez Créer un groupe de facturation.

> Remarques
>
> - Vous devez sélectionner votre compte principal à l'étape 9. Vous ne pouvez pas modifier votre compte principal une fois le groupe de facturation créé. Pour attribuer un nouveau compte principal, supprimez le groupe de facturation et regroupez vos comptes. Bien qu'un compte payeur puisse être inclus dans un groupe de facturation, le rôle du compte principal ne peut pas être attribué à un compte payeur.
> - Si le compte principal d'un groupe de facturation quitte votre organisation et que l'association automatique de comptes est activée pour ce groupe de facturation, il continuera à associer automatiquement les comptes jusqu'à la fin du mois. Ensuite, le groupe de facturation sera automatiquement supprimé. Vous pouvez activer l'association automatique de comptes pour un groupe de facturation existant ou en créer un autre.

Tableau des groupes de facturation

Après avoir créé un groupe de facturation, vous pouvez consulter les détails du groupe de facturation dans un tableau filtrable. Vous pouvez filtrer en utilisant les dimensions suivantes :

- Nom du groupe de facturation
- Nom du compte principal
- ID du compte principal
- Nombre de comptes
- Nom du plan tarifaire

Pour consulter les détails de chaque groupe de facturation, choisissez le nom du groupe de facturation dans le tableau. Le groupe de facturation que vous avez activé pour la fonctionnalité d'association automatique de comptes aura une icône d'association automatique à côté du nom du groupe de facturation.

Création de règles de tarification

Vous pouvez créer des règles de tarification dans AWS Billing Conductor afin de personnaliser vos taux de facturation dans tous vos groupes de facturation. Les règles de tarification peuvent être globales, spécifiques au service, spécifiques à l'entité de facturation ou spécifiques au SKU. Vous pouvez utiliser les règles de tarification pour appliquer une réduction ou une majoration pour chaque étendue respective. Les portées ne se chevauchent pas. Les champs d'application sont appliqués de la manière la plus précise à la plus précise lorsque des règles de tarification ayant des portées différentes sont contenues dans un seul plan tarifaire. Pour les règles tarifaires internationales, vous pouvez également choisir de désactiver ou d'activer `Always Free Tier` les tarifs. Les règles tarifaires avec le niveau Always Free désactivé s'appliquent par défaut au premier niveau payant pour le type d'utilisation ou l'opération. Par défaut, un compte payeur doté d'autorisations d'administrateur peut créer des règles de tarification. Il faut jusqu'à 24 heures après l'application d'une règle de tarification à un groupe de facturation pour que les tarifs personnalisés de votre groupe de facturation soient pris en compte.

Un seul plan tarifaire peut être appliqué à plusieurs groupes de facturation.

Suivez les étapes ci-dessous pour créer une règle de tarification.

Pour créer une règle de tarification

1. Ouvrez AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, choisissez Configuration des prix.
3. Choisissez l'onglet Règles de tarification.
4. Choisissez Créer des règles de tarification.
5. Pour les détails des règles de tarification, entrez le nom de la règle de tarification. Pour les restrictions de dénomination, voirQuotas et restrictions.
6. (Facultatif) Dans Description, entrez une description pour la règle de tarification.
7. Pour ÉtendueGlobal, sélectionnez `ServiceBilling entity`, ouSKU.

   - Global : s'applique à tous les usages.
   - Service : s'applique uniquement à un service donné. Lorsque vous choisissez un service, choisissez un code de service pour lequel configurer les tarifs. Lorsque vous choisissez un service, choisissez le code de service que vous souhaitez ajuster dans l'API Price List Query.

- Entité de facturation : s'applique uniquement à une entité de facturation donnée. Une entité de facturation est le vendeur de services fournis par AWS, ses filiales ou des fournisseurs tiers qui vendent des services par l'intermédiaire de ceux-ci AWS Marketplace.
- SKU : s'applique uniquement à la combinaison unique du code de service (produit), du type d'utilisation et/ou de l'opération.

8. Dans Type, choisissez Discount, Markup ou Tiering.

> **Note**
>
> La hiérarchisation n'est disponible que pour les règles de tarification globales et spécifiques aux services.

9. Dans Pourcentage, entrez le montant en pourcentage.

   Si vous entrez **0** un pourcentage, le plan tarifaire utilise par défaut le tarif à la AWS demande. Si vous entrez une valeur décimale, elle sera arrondie à la deuxième décimale la plus proche.

10. Pour le type de hiérarchisation, vous pouvez cocher la case sous Configuration de la hiérarchisation pour désactiver le niveau Always Free, ou le laisser tel quel. Le niveau Always Free sera activé sauf s'il est explicitement désactivé.
11. (Facultatif) Pour créer une autre règle de tarification dans le même flux de travail, choisissez Ajouter une règle de tarification.
12. Choisissez Créer une règle de tarification.

Tableau des règles de tarification

Après avoir créé une règle de tarification, vous pouvez consulter les détails de la règle de tarification dans un tableau filtrable. Vous pouvez filtrer selon les dimensions suivantes :

- Nom de la règle de tarification
- Portée
- Type
- Détails
- Vitesse

Création de plans de tarification

Vous pouvez créer des plans tarifaires dans AWS Billing Conductor pour personnaliser la sortie de vos informations de facturation dans tous vos groupes de facturation. Par défaut, un compte payeur doté d'autorisations d'administrateur peut créer des plans tarifaires. Il faut jusqu'à 24 heures après l'application d'un plan tarifaire à un groupe de facturation pour que les tarifs personnalisés de votre groupe de facturation soient pris en compte.

Un seul plan tarifaire peut être appliqué à plusieurs groupes de facturation.

> **Note**
>
> La mise à jour d'un plan tarifaire affecte également les détails de facturation de chaque groupe de facturation auquel le plan tarifaire est associé. Si le plan tarifaire est associé à un groupe de facturation ou à un ensemble de groupes de facturation, cette modification n'affecte que la période de facturation en cours. Les périodes de facturation précédentes restent inchangées.

Suivez les étapes ci-dessous pour créer un plan tarifaire.

Pour créer un plan tarifaire

1. Ouvrez AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, choisissez Configuration des prix.
3. Dans l'onglet Plan tarifaire, choisissez Créer un plan tarifaire.
4. Pour les détails du plan tarifaire, entrez le nom du plan tarifaire. Pour les restrictions de dénomination, voirQuotas et restrictions.
5. (Facultatif) Dans Description, entrez une description du plan tarifaire.
6. Dans le tableau des règles de tarification, choisissez les règles de tarification que vous souhaitez associer au plan tarifaire. Vous pouvez filtrer les règles de tarification par nom, champ d'application, détails, type ou taux des règles de tarification.
7. Choisissez Créer un plan tarifaire.

Tableau du plan tarifaire

Après avoir créé un plan tarifaire, vous pouvez consulter les détails du plan tarifaire dans un tableau filtrable. Vous pouvez filtrer selon les dimensions suivantes :

- Le nom du plan tarifaire
- La description
- Le nombre de règles de tarification associées au plan tarifaire

Création de postes personnalisés par groupe de facturation

Utilisez-le AWS Billing Conductor pour créer des rubriques personnalisées et les appliquer à des rubriques désignées Comptes AWS au sein d'un groupe de facturation.

Vous pouvez répartir les coûts et les remises en utilisant des rubriques personnalisées. Vous pouvez calculer un article personnalisé sous forme de frais forfaitaire ou de pourcentage de frais. Configurez l'élément de ligne personnalisé basé sur le pourcentage pour inclure ou exclure des ressources. Ces ressources incluront les coûts des groupes de facturation et d'autres éléments fixes personnalisés associés à un groupe de facturation pour une période de facturation. Vous pouvez ensuite définir les rubriques personnalisées pour qu'elles s'appliquent pendant un mois ou qu'elles se reproduisent pendant plusieurs mois.

Les cas d'utilisation courants pour la création d'éléments de ligne personnalisés incluent, sans toutefois s'y limiter, les suivants :

- Allocation des frais AWS Support
- Répartition des coûts des services partagés
- Appliquer des frais de service gérés
- Appliquer la taxe
- Distribution de crédits
- Répartir les économies réalisées sur le RI et les Savings Plans (par opposition à On-Demand)
- Ajouter des crédits organisationnels et des éléments de ligne de réduction

Création d'un article personnalisé à tarif fixe

Suivez les étapes ci-dessous pour créer une ligne personnalisée qui applique une ligne de crédit ou de frais à un groupe de facturation individuel.

Pour créer un article personnalisé

1. Ouvrez AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, sélectionnez Éléments de ligne personnalisés.
3. Choisissez Créer un article personnalisé.
4. Pour les détails du poste personnalisé, entrez le nom du poste personnalisé. Pour les restrictions de dénomination, voirQuotas et restrictions.
5. Dans Description, entrez une description pour le poste personnalisé. La limite de caractères est de 255.
6. Pour Période de facturation, choisissez la période de facturation existante ou la période de facturation précédente.
7. Pour Durée, choisissez un mois ou une durée récurrente (aucune date de fin définie).
8. Pour Groupe de facturation, choisissez un groupe de facturation. Vous ne pouvez associer les frais personnalisés qu'à un seul groupe de facturation à la fois.

    - (Facultatif) Pour le compte alloué, vous pouvez appliquer votre rubrique personnalisée au compte du groupe de facturation de votre choix. Votre article personnalisé est appliqué par défaut au compte principal du groupe de facturation de votre choix.
9. Choisissez Forfait pour votre type de rubrique personnalisé.
10. Choisissez un type de charge et entrez un montant d'entrée.

    Un article de la ligne de discount ajoute un crédit. Cela réduit le montant facturé au groupe de facturation sélectionné. Un élément de ligne d'annotation ajoute des frais. Cela augmente le montant facturé au groupe de facturation sélectionné. Tous les articles personnalisés sont en dollars américains.
11. Choisissez Créer.

Création d'une rubrique personnalisée facturée en pourcentage

Suivez les étapes ci-dessous pour créer une ligne personnalisée qui applique une ligne de crédit ou de frais à un groupe de facturation individuel.

Pour créer un article personnalisé

1. Ouvrez AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, sélectionnez Éléments de ligne personnalisés.
3. Choisissez Créer un article personnalisé.
4. Pour les détails du poste personnalisé, entrez le nom du poste personnalisé. Pour les restrictions de dénomination, voirQuotas et restrictions.
5. Dans Description, entrez une description pour le poste personnalisé. La limite de caractères est de 255.
6. Pour Période de facturation, choisissez la période de facturation existante ou la période de facturation précédente.
7. Pour Durée, choisissez un mois ou une durée récurrente (aucune date de fin définie).
8. Pour Groupe de facturation, choisissez un groupe de facturation. Vous ne pouvez associer les frais personnalisés qu'à un seul groupe de facturation à la fois.

    - (Facultatif) Pour le compte alloué, vous pouvez appliquer votre rubrique personnalisée au compte du groupe de facturation de votre choix. Votre article personnalisé est appliqué par défaut au compte principal du groupe de facturation de votre choix.
9. Choisissez le pourcentage de frais pour votre type de rubrique personnalisé.
10. Choisissez un type de charge et entrez un montant d'entrée.

    Un article de la ligne de discount ajoute un crédit. Cela réduit le montant facturé au groupe de facturation sélectionné. Un élément de ligne d'annotation ajoute des frais. Cela augmente le montant facturé au groupe de facturation sélectionné. Tous les articles personnalisés sont en dollars américains.
11. (Facultatif) Pour les valeurs des ressources, choisissez les valeurs à inclure dans le calcul. Par défaut, le coût total du groupe de facturation est sélectionné comme ressource. Cela exclut tous les articles de gamme personnalisés plats.

    - (Facultatif) Par défaut, les remises du Savings Plan sont incluses. Pour les exclure du calcul, cochez la case Exclure les remises du Savings Plan.
12. (Facultatif) Incluez un ou plusieurs articles personnalisés plats. Choisissez chaque ligne personnalisée plate applicable dans le tableau que vous souhaitez inclure dans le calcul basé sur le pourcentage.

> **Note**
>
> Vous pouvez créer des rubriques personnalisées en pourcentage sans ressources associées. Ces rubriques personnalisées indiquent une `$0.00` valeur dans vos données de facturation.

13. Choisissez Créer.

Tableau des articles personnalisés

Après avoir créé un élément de ligne personnalisé, vous pouvez afficher les détails du poste dans un tableau filtrable. Vous pouvez filtrer selon les dimensions suivantes :

- Le nom de l'élément de ligne
- Description de la rubrique
- Le montant facturé
- Le groupe de facturation auquel le poste est attribué
- Date de création de cette rubrique

Pour afficher les articles personnalisés que vous avez créés au cours des périodes de facturation précédentes, utilisez la liste déroulante du sélecteur de dates.

Modification d'éléments de ligne personnalisés

Suivez les étapes ci-dessous pour modifier vos articles personnalisés.

Pour modifier un élément de ligne personnalisé

1. Ouvrez AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, sélectionnez Éléments de ligne personnalisés.
3. Choisissez Créer un article personnalisé.
4. Choisissez l'élément de ligne personnalisé que vous souhaitez modifier.
5. Choisissez Modifier.
6. Modifiez les paramètres souhaités.

> **Note**
>
> Vous ne pouvez pas modifier la période de facturation, le groupe de facturation, le compte attribué, le type de frais (forfaitaire ou pourcentage) ou le type de valeur de facturation (crédit ou frais).

7. Sélectionnez Enregistrer les modifications.

Supprimer des éléments de ligne personnalisés

Suivez les étapes ci-dessous pour supprimer vos articles personnalisés.

Pour modifier un élément de ligne personnalisé

1. Ouvrez AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, sélectionnez Éléments de ligne personnalisés.
3. Choisissez Créer un article personnalisé.
4. Choisissez l'élément de ligne personnalisé que vous souhaitez supprimer.
5. Choisissez Supprimer.
6. Découvrez comment la suppression de l'élément personnalisé peut vous affecter, puis choisissez Supprimer le poste personnalisé.

Meilleures pratiques pour AWS Billing Conductor

Cette section présente certaines des meilleures pratiques à appliquer lorsque vous travaillez avec AWS Billing Conductor.

Rubriques

Comprendre l'importance de la date d'adhésion au compte principal

La date à laquelle le compte principal a rejoint votre organisation définit la limite historique des coûts pro forma pour ce groupe de facturation. Si vous choisissez un compte principal créé ou associé à votre compte de gestion au milieu du mois, les coûts pro forma n'incluront pas les coûts des autres comptes du groupe de facturation, y compris les comptes qui faisaient partie de votre organisation avant l'adhésion du compte principal.

Supposons, par exemple, que le compte principal ait rejoint votre organisation le 15 octobre. La facture pro forma pour tous les comptes du groupe de facturation inclura uniquement le coût et l'utilisation à compter de cette date. La facture pro forma commence le 15 octobre, même si d'autres comptes du groupe de facturation étaient membres de l'organisation avant le mois en cours.

Il y aura un écart entre le domaine de facturation facturable et le domaine de facturation pro forma pour le premier mois du groupe de facturation. Le domaine pro forma n'inclura aucune utilisation accumulée avant le 15 octobre. Après le premier mois, les coûts pro forma refléteront toutes les utilisations.

Pour éviter cet écart initial entre les données facturables et les données pro forma figurant dans la première facture du groupe de facturation, choisissez un compte principal lié au compte de gestion pendant tout le mois ou avant.

Contrôle de l'accès à AWS Billing Conductor

Le Billing and Cost Management n'est accessible qu'aux utilisateurs ayant accès au payeur ou au compte de gestion. Pour autoriser les utilisateurs IAM à créer des groupes de facturation et à consulter les indicateurs de performance clés (KPI) de AWS Billing Conductor dans la console Billing and Cost Management, vous devez également accorder aux utilisateurs IAM les avantages suivants :

- Répertorier les comptes au sein d'Organizations

Pour en savoir plus sur la possibilité pour les utilisateurs de créer des groupes de facturation et des plans tarifaires dans la console AWS Billing Conductor, consultezGestion des identités et des accès pour AWS Billing Conductor.

Vous pouvez également créer des ressources AWS Billing Conductor par programmation à l'aide de l'API AWS Billing Conductor. Lorsque vous configurez l'accès à l'API AWS Billing Conductor, nous vous recommandons de créer un utilisateur IAM unique pour autoriser l'accès programmatique. Cela vous permet de définir des contrôles d'accès plus précis entre les personnes de votre organisation ayant accès à la console AWS Billing Conductor et à l'API. Pour permettre à plusieurs utilisateurs IAM d'accéder par requête à l'API AWS Billing Conductor, nous recommandons de créer un rôle IAM d'accès programmatique pour chacun d'entre eux.

Comprendre l'ensemble de données AWS Billing Conductor

Bien que les modèles de données AWS Billing Conductor présentent de nombreuses similitudes avec le modèle AWS de données de facturation standard, il existe quelques différences.

Le AWS responsable de la facturation n'inclut pas :

- Crédits (utilisés au niveau du payeur ou du compte lié)
- Taxes
- AWS Support frais

En outre, le AWS Billing Conductor partage les instances réservées et les Savings Plans avec les comptes placés dans le même groupe de facturation, quelles que soient vos préférences de partage dans le domaine de facturation standard.

Comprendre la logique de calcul AWS de Billing Conductor

Le calcul du directeur AWS de facturation est flexible en fonction des modifications que vous apportez au cours d'un mois donné, tout en préservant l'intégrité historique de vos données de facturation de la période précédente. Il est préférable de le décrire à l'aide d'un exemple.

Dans cet exemple, nous avons deux groupes de facturation, `A` et`B`. Le groupe de facturation `A` commence la période de facturation avec les comptes 1 à 3 du groupe. Au milieu du mois, le compte du payeur passe `Account 3` à`Billing Group B`. À ce stade, le recalcul des coûts pour les groupes `A` de facturation est nécessaire pour modéliser avec précision le dernier changement. `B` Lorsqu'il `Account 3` est déplacé, `Billing Group A` son utilisation est modélisée comme si elle ne `Account 3` faisait pas partie du groupe de facturation pendant la période de facturation en cours. De plus, `Billing Group B` son utilisation est modélisée comme si `Account 3` elle en faisait partie `Billing Group B` depuis le début de la période de facturation. Cette approche élimine le besoin de calculer des taux complexes et des modèles de rétrofacturation lorsque les comptes passent d'un groupe à un autre au cours de la période de facturation.

Groupe de facturation A	Jours : 1 à 15	Jours : 16 à 30	Fin du mois
Compte 1	100$	100$	200$
Compte 2	100$	100$	200$
Compte 3	100$	N/A	N/A
Total	300$	200$	400$

Groupe de facturation B	Jours : 1 à 15	Jours : 16 à 30	Fin du mois
Compte 4	100$	100$	200$
Compte 5	100$	100$	200$
Compte 6	100$	100$	200$

Groupe de facturation B	Jours : 1 à 15	Jours : 16 à 30	Fin du mois
Compte 3	100$	100$	200$
Total	400$	400$	800$

Comprendre la fréquence de mise à jour AWS de Billing Conductor

AWS les données de facturation sont mises à jour au moins une fois par jour. AWS Billing Conductor utilise ces données pour calculer vos données de facturation pro forma. Les rubriques personnalisées générées pour s'appliquer au mois en cours sont reflétées dans les 24 heures. Les articles personnalisés générés pour s'appliquer à la période de facturation précédente peuvent prendre jusqu'à 48 heures pour être reflétés dans les rapports sur les AWS coûts et l'utilisation d'un groupe de facturation, ou sur la page des factures d'un groupe de facturation donné.

Comprendre les différences entre le AWS CUR AWS de Billing Conductor et le AWS CUR standard

Il existe quelques différences entre les rapports de coûts et d'utilisation standard et le AWS CUR pro forma créé à l'aide de la configuration AWS de Billing Conductor.

- Le AWS CUR standard calcule le coût et l'utilisation de chaque compte de votre famille de facturation consolidée. Un AWS CUR pro forma par groupe de facturation inclut uniquement les comptes du groupe de facturation au moment du calcul.
- Le AWS CUR standard remplit la colonne de facture une seule fois et la facture est générée par AWS. Un AWS CUR pro forma ne remplit pas la colonne de facture. Actuellement, aucune facture n'est générée ou émise sur la AWS base des données de facturation pro forma.

Analyse de vos marges par groupe de facturation

Vous pouvez utiliser le résumé et le détail des marges dans AWS Billing Conductor pour analyser vos marges à la fois globalement et avec des groupes de facturation spécifiques.

Suivez les étapes ci-dessous pour consulter vos marges pour un groupe de facturation individuel ou un ensemble de groupes de facturation.

Rubriques

Visualisez vos marges dans leur ensemble à l'aide du résumé des marges

Pour consulter le récapitulatif des marges de votre groupe de facturation

1. Ouvrez AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, sous Analytics, sélectionnez Résumé des marges.
3. Pour Type de rapport, choisissez Tous les groupes de facturation ou Sélectionnez le groupe de facturation.
4. Si vous avez choisi Sélectionner les groupes de facturation, choisissez une période de facturation et un ou plusieurs groupes de facturation.
5. Dans la section onth-to-date d'aperçu M, vous pouvez consulter le montant facturé, AWS les coûts et la marge.
6. Vous pouvez consulter l'analyse de vos marges de deux manières :
   - Sous forme de graphique à barres dans la section Performances (jusqu'aux 13 derniers mois).
   - Sous forme de tableau dans le tableau d'analyse des marges.

   Les marges négatives sont indiquées en rouge sur le graphique, avec un montant négatif en dollars et un pourcentage négatif.

Comprendre votre tableau d'analyse des marges

Le tableau d'analyse des marges du groupe de facturation est trié par ordre chronologique inverse par défaut. Vous pouvez trier le tableau en fonction de toutes les colonnes, notamment les suivantes :

- Mois
- Montant facturé
- AWS coûts
- Montant de la marge
- Pourcentage de marge

Le graphique et le tableau renvoient les valeurs des 13 derniers mois pour les groupes de facturation sélectionnés. Si les groupes de facturation ont été créés à des moments différents, nous partons de la plage horaire du plus ancien groupe de facturation sélectionné.

Vous pouvez exporter votre tableau d'analyse des marges vers un fichier CSV téléchargeable. À côté de votre tableau d'analyse des marges, choisissez Télécharger le fichier CSV. Votre téléchargement démarrera automatiquement.

> **Note**
>
> Pour télécharger un fichier CSV contenant l'analyse des marges de votre groupe de facturation, l'`billingconductor:ListBillingGroupCostReport`autorisation doit être ajoutée à votre politique IAM.

Consultez vos marges Service AWS par en utilisant le détail des marges

Pour consulter les marges de votre groupe de facturation par service

1. Ouvrez AWS Billing Conductor à l'adresse https://console.aws.amazon.com/billingconductor/.
2. Dans le volet de navigation, sous Analytics, sélectionnez Détails de la marge.
3. Sous Paramètres du rapport, choisissez une période de facturation et un groupe de facturation.
4. Vous pouvez consulter l'analyse de vos marges de deux manières :

- Sous forme de graphique linéaire dans la section Tendance des marges par les 5 principaux services.
- Sous forme de tableau dans le tableau d'analyse des marges.

Comprendre le graphique des tendances de vos marges

Le détail de vos marges affichera un graphique linéaire qui affiche les cinq meilleurs services par marge pour la période de facturation choisie. Le graphique linéaire affichera les marges de chaque service au cours des trois derniers mois à des fins de comparaison.

Le graphique comprendra également un tableau qui affiche les marges de chaque service pour la période de facturation choisie. Le tableau affiche la marge moyenne calculée au cours des trois derniers mois, qui comprend les colonnes suivantes :

- Nom du service
- Moyenne
- Marge

Si le groupe de facturation n'a pas été actif pendant l'intégralité des trois derniers mois, le graphique n'affichera que les données du rapport de coûts disponibles.

Comprendre votre tableau d'analyse des marges

Le tableau d'analyse des marges du groupe de facturation comprend les colonnes suivantes :

- Nom du service
- Montant facturé
- AWS coûts
- Montant de la marge
- Pourcentage de marge

Vous pouvez exporter votre tableau d'analyse des marges vers un fichier CSV téléchargeable. À côté de votre tableau d'analyse des marges, choisissez Télécharger le fichier CSV. Votre téléchargement démarrera automatiquement.

> **Note**
>
> Pour télécharger un fichier CSV contenant l'analyse des marges de votre groupe de facturation, l'`billingconductor:GetBillingGroupCostReport`autorisation doit être ajoutée à votre politique IAM.

Affichage des détails de votre groupe de facturation

Vous pouvez utiliser les détails de votre groupe de facturation pour surveiller, analyser et modifier votre groupe de AWS facturation dans Billing Conductor. Les détails du groupe de facturation fournissent une analyse des month-to-date marges, un historique des rubriques personnalisées appliquées et la possibilité de modifier et de supprimer le groupe de facturation selon les besoins.

Affichage de vos informations de facturation par dimensions de prix personnalisées

Une fois que vous avez créé et attribué vos groupes de facturation et vos plans tarifaires, vous pouvez consulter vos dimensions de facturation personnalisées avec la granularité des types d'utilisation pour chaque groupe de facturation géré.

Procédez comme suit pour consulter vos informations de facturation dans le domaine pro forma.

Pour consulter vos informations de facturation pro forma

1. Ouvrez la AWS Billing console à l'adresse https://console.aws.amazon.com/billing/.
2. Dans le volet de navigation, choisissez Factures.
3. Choisissez Paramètres dans le coin supérieur droit des informations de facturation.
4. Activez l'affichage des données Pro forma.
5. Pour le groupe de facturation, choisissez la facturation à analyser.

Vous pouvez analyser l'utilisation du groupe de facturation par service et par AWS région pour connaître le coût de cette utilisation, conformément aux tarifs définis dans AWS Billing Conductor.

Vous pouvez trouver les rubriques personnalisées sous le service AWSBilling Conductor sur la page des détails de facturation.

Configuration des rapports de coûts et d'utilisation par groupe de facturation

Vous pouvez créer des rapports de AWS coûts et d'utilisation (AWSCUR) pro forma pour chaque groupe de facturation que vous créez. Le AWS CUR pro forma possède le même format de fichier, la même granularité et les mêmes colonnes que le AWS CUR standard et contient l'ensemble le plus complet de données sur les coûts et l'utilisation disponibles pour une période donnée.

Vous pouvez publier votre AWS CUR pro forma dans un compartiment Amazon Simple Storage Service (Amazon S3) dont vous êtes le propriétaire.

AWSmet à jour le rapport dans votre bucket une fois par jour dans des valeurs séparées par des virgules (CSV) ou au format Apache Parquet. Vous pouvez consulter les rapports à l'aide de tableurs tels que Microsoft Excel et Apache OpenOffice Calc. Vous pouvez également y accéder depuis une application à l'aide des API Amazon S3 ou Amazon Athena. Pour plus d'informations sur le AWS CUR standard, consultez le Guide de l'utilisateur des rapports de AWS coûts et d'utilisation.

Procédez comme suit pour générer un AWS CUR pro forma pour un groupe de facturation.

Pour créer des rapports de coûts et d'utilisation pro forma pour un groupe de facturation

1. Ouvrez la AWS Billing console à l'adresse https://console.aws.amazon.com/billing/.
2. Dans le volet de navigation, choisissez Rapports sur les coûts et l'utilisation.
3. En haut à droite du tableau du rapport, choisissez Paramètres.
4. Activez l'affichage des données Pro forma.
5. Sélectionnez Enable (Activer).
6. Choisissez Créer un rapport.
7. Pour Nom du rapport, entrez un nom pour votre rapport.
8. Pour l'affichage des données, choisissez pro forma.
9. Pour le groupe de facturation, choisissez un groupe de facturation.
10. Pour Additional report details (Autres détails sur le rapport), sélectionnez Include resource IDs (Inclure les ID de ressource) si vous souhaitez inclure l'ID de chaque ressource dans le rapport.
11. Pour les paramètres d'actualisation des données, indiquez si vous souhaitez que les rapports de AWS coûts et d'utilisation soient actualisés en fonction de toute nouvelle modification apportée

à vos données de coût et d'utilisation après la finalisation de votre facture. Lorsqu'un rapport est actualisé, un nouveau rapport est chargé sur Amazon S3.

> **Note**
>
> Les rapports sur les coûts et l'utilisation des groupes de facturation n'incluent pas les crédits, les taxes ou les frais d'assistance.

12. Choisissez Suivant.
13. Pour Compartiment S3, choisissez Configurer.
14. Dans la boîte de dialogue Configure S3 Bucket (Configurer le compartiment S3), exécutez l'une des actions suivantes :

    - Choisissez un bucket existant dans la liste déroulante, puis choisissez Suivant.
    - Entrez un nom de compartiment et la AWS région dans laquelle vous souhaitez créer un nouveau compartiment, puis choisissez Suivant.
15. Sélectionnez J'ai confirmé que cette politique est correcte, puis cliquez sur Enregistrer.
16. Pour Préfixe du chemin de rapport, entrez le préfixe de chemin que vous souhaitez ajouter devant le nom de votre rapport.

    Cette étape est facultative pour Amazon Redshift ou AmazonQuickSight, mais obligatoire pour Amazon Athena.

    Si vous ne spécifiez aucun préfixe, le préfixe par défaut est le nom que vous spécifiez pour le rapport à l'étape 4 et la plage de dates du rapport au format suivant :

    ```
    /report-name/date-range/
    ```
17. Pour Time granularity (Granularité temporelle), choisissez l'une des options suivantes :

    - Hourly (Par heure) si vous souhaitez que les postes du rapport soient regroupés par heure.
    - Daily (Par jour) si vous souhaitez que les postes du rapport soient regroupés par jour.
18. Pour Report versioning (Gestion des versions du rapport), précisez si vous voulez que chaque version du rapport remplace sa version précédente ou si elle doit être remise en plus de la version précédente.
19. Pour Activer l'intégration des données des rapports pour, choisissez si vous souhaitez charger vos rapports de coûts et d'utilisation sur Amazon Athena, Amazon Redshift ou Amazon. QuickSight Le rapport est compressé dans les formats suivants :

- Athena : compression de parquet
- Amazon Redshift ou Amazon QuickSight : compression .gz

20. Choisissez Suivant.
21. Après avoir vérifié les paramètres de votre rapport, choisissez Réviser et terminer.

Réalisation d'une analyse ad hoc sur les coûts pro forma dans AWS Cost Explorer

Comptes AWSdans Billing Conductor, les groupes de facturation peuvent analyser, prévoir et signaler les coûts pro forma dans Cost Explorer. Le compte principal d'un groupe de facturation peut effectuer ces activités pour tous les comptes du groupe. Si vous utilisezAWS Organizations, les comptes de gestion ne peuvent pas analyser, prévoir ou signaler les coûts pro forma dans Cost Explorer.

Les comptes gérés par le groupe de facturation (membres du groupe de facturation) peuvent consulter les données de coût et d'utilisation pour les périodes de facturation pendant lesquelles ils étaient membres du groupe de facturation, et les données pro forma sont disponibles. Ils ne peuvent pas consulter l'historique des coûts facturables et des données d'utilisation.

Remarques

- Les comptes gérés par Billing Conductor (membres du groupe de facturation) peuvent consulter les coûts pro forma dans Cost Explorer.
- Les données de granularité horaire ne sont pas prises en charge par les coûts pro forma dans Cost Explorer.
- Pour en savoir plus sur les principaux flux de travail pris en charge par Cost Explorer, consultez la section Exploration de vos données à l'aide de Cost Explorer dans le guide de AWS Cost Management l'utilisateur.

Pour obtenir la liste Services AWS des coûts pro forma de ce support, voirServices AWS qui prennent en charge les coûts pro forma.

Services AWS qui prennent en charge les coûts pro forma

Les services de gestion financière dans le cloud suivants et leurs fonctionnalités prennent en charge les coûts pro forma.

Service et fonctionnalités	Support par Compte AWS type		
	Payeur (compte de gestion)	Compte principal	Lié (compte membre)
AWS Cost and Usage Report	Oui	Oui	Oui
Répartition des coûts fractionnée	Non	Non	Non
AWS Billing	Non	Oui	Oui
Tableau de bord	Non	Oui	Oui
Détails relatifs à la facturation	Oui	Oui	Oui
Télécharger le fichier CSV	Non	Non	Non
AWS Cost Explorer	Non	Oui	Oui
Prévisions	Non	Oui	Oui
Enregistrer les rapports	Non	Oui	Oui
Recommandations de dimensionnement	Non	Non	Non
Surveillance des anomalies de coûts	Non	Non	Non

Service et fonctionnalités	Support par Compte AWS type		
Recommandations relatives à Savings Plans	Non	Non	Non
Rapports d'utilisation de Savings Plans	Non	Non	Non
Rapports de couverture de Savings Plans	Non	Non	Non
Recommandations de réservation	Non	Non	Non
Rapports sur l'utilisation des réservations	Non	Non	Non
Rapports sur la couverture des réservations	Non	Non	Non
AWS Budgets	Non	Non	Non
Rapports budgétaires	Non	Non	Non

Pour les services et fonctionnalités qui ne prennent pas en charge les coûts pro forma, les coûts Comptes AWS seront facturés aux taux facturables, qui correspondent à la AWS facture.

Informations connexes

Pour gérer l'accès aux comptes associés aux remboursements, crédits et remises facturables, consultez la AWS Cost Explorersection de la page Préférences de la console de gestion des coûts.

Si vous ne souhaitez pas que vos entités IAM bénéficient de tarifs facturables spécifiques pour ces services et fonctionnalités, vous pouvez utiliser les politiques IAM pour refuser l'accès. Pour obtenir un exemple de politique IAM, consultez Refuser à Billing et à Cost Explorer l'accès aux services et fonctionnalités qui ne prennent pas en charge les coûts pro forma.

Vous pouvez également personnaliser vos politiques IAM pour autoriser ou refuser des autorisations spécifiques. Pour obtenir une liste détaillée des actions IAM pour Billing and Cost Management, consultez les rubriques suivantes :

- Migration du contrôle d'accès pour le AWS Cost Management guide de l'AWS Cost Management utilisateur
- Migration du contrôle d'accès pour AWS Billing et dans le guide de l'AWS Billing utilisateur

Utilisation de l'API AWS Billing Conductor

L'API Billing Conductor est disponible en Java, Python, .NET et Go. Les nouvelles fonctionnalités publiées dans Billing Conductor seront également disponibles sous forme d'API.

Pour plus d'informations sur leAWSAPI Billing Conductor, consultez leAWS Billing ConductorRéférence d'API.

Sécurité dans AWS Billing Conductor

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Billing Conductor, consultez la section Services AWS concernés par programme de conformité .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS Billing Conductor. Les rubriques suivantes expliquent comment configurer AWS Billing Conductor pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS qui vous aident à surveiller et à sécuriser vos ressources AWS Billing Conductor.

Rubriques

Protection des données dans AWS Billing Conductor

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans AWS Billing Conductor. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AWS Billing Conductor ou un autre utilisateur Services AWS à l'aide de la console AWS CLI, de l'API ou AWS des SDK. Toutes

les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Gestion des identités et des accès pour AWS Billing Conductor

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de Billing Conductor. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Billing Conductor.

Utilisateur du service : si vous utilisez le service Billing Conductor pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de Billing Conductor pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Billing Conductor, consultezRésolution des problèmes AWS Billing Conductor d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des ressources de Billing Conductor dans votre entreprise, vous avez probablement un accès complet à Billing Conductor. C'est à vous de déterminer les fonctionnalités et les ressources de Billing Conductor auxquelles les utilisateurs du service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Billing Conductor, consultezComment AWS Billing Conductor fonctionne avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Billing Conductor. Pour consulter des exemples de politiques basées sur l'identité de Billing Conductor que vous pouvez utiliser dans IAM, consultez. AWS Billing Conductor exemples de politiques basées sur l'identité

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, veuillez consulter Multi-factor authentication (Authentification multifactorielle) dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Utilisateur racine d'un compte AWS

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant les informations d'identification de l'utilisateur root dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent

des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, veuillez consulter la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte – Vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction de service ou un rôle lié au service.

- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
- Fonction du service – Il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal

(utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Présentation des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de

confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations – Une limite d'autorisations est une fonction avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations qui en résultent représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance – Les politiques de séance sont des politiques avancées que vous passez en tant que paramètre lorsque vous programmez afin de créer une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la séance obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Billing Conductor fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Billing Conductor, vous devez connaître les fonctionnalités IAM disponibles avec Billing Conductor. Pour obtenir une vue d'ensemble de la façon dont Billing Conductor et les autres AWS services fonctionnent avec IAM, consultez la section AWS Services qui fonctionnent avec IAM dans le guide de l'utilisateur d'IAM.

Rubriques

- Politiques basées sur l'identité de Billing Conductor
- Politiques basées sur les ressources de Billing Conductor
- Listes de contrôle d'accès (ACL)
- Autorisation basée sur les tags Billing Conductor

- Rôles IAM de Billing Conductor

Politiques basées sur l'identité de Billing Conductor

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Billing Conductor prend en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, veuillez consulter Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique dans Billing Conductor utilisent le préfixe suivant avant l'action :`Billing Conductor:`. Par exemple, pour accorder à une personne l'autorisation d'exécuter une instance Amazon EC2 avec l'opération d'API `RunInstances` Amazon EC2, vous incluez l'action `ec2:RunInstances` dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Billing Conductor définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "ec2:Describe*"
```

Pour consulter la liste des actions de Billing Conductor, consultez la section Actions définies par AWS Billing Conductor dans le guide de l'utilisateur d'IAM.

Ressources

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets pour lesquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

La ressource d'instance Amazon EC2 possède l'ARN suivant :

```
arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}
```

Pour plus d'informations sur le format des ARN, consultez Amazon Resource Names (ARN) et AWS Service Namespaces.

Par exemple, pour spécifier l'instance `i-1234567890abcdef0` dans votre instruction, utilisez l'ARN suivant :

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Pour spécifier toutes les instances qui appartiennent à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Certaines actions de Billing Conductor, telles que celles relatives à la création de ressources, ne peuvent pas être effectuées sur une ressource spécifique. Dans ce cas, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

De nombreuses actions d'API Amazon EC2 nécessitent plusieurs ressources. Par exemple, comme `AttachVolume` attache un volume Amazon EBS à une instance, un utilisateur IAM doit avoir les autorisations nécessaires pour utiliser le volume et l'instance. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
```

Pour consulter la liste des types de ressources Billing Conductor et leurs ARN, consultez la section Ressources définies par AWS Billing Conductor dans le guide de l'utilisateur IAM. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez la section Actions définies par AWS Billing Conductor.

Clés de condition

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR`

opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Billing Conductor définit son propre ensemble de clés de condition et prend également en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, consultez la section Clés contextuelles de condition AWS globale dans le guide de l'utilisateur IAM.

Toutes les actions Amazon EC2 prennent en charge les clés de condition `aws:RequestedRegion` et `ec2:Region`. Pour de plus amples informations, veuillez consulter Exemple : Restriction de l'accès à une région spécifique.

Pour consulter la liste des clés de condition de Billing Conductor, voir Clés de condition pour AWS Billing Conductor dans le guide de l'utilisateur d'IAM. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir Actions définies par AWS Billing Conductor.

Exemples

Pour consulter des exemples de politiques basées sur l'identité de Billing Conductor, consultez. AWS Billing Conductor exemples de politiques basées sur l'identité

Politiques basées sur les ressources de Billing Conductor

Les politiques basées sur les ressources sont des documents de politique JSON qui spécifient les actions qu'un principal spécifié peut effectuer sur la ressource Billing Conductor et dans quelles conditions. *Amazon S3 prend en charge les politiques d'autorisation basées sur les ressources pour les compartiments Amazon S3.* Les politiques basées sur les ressources permettent d'accorder une autorisation à d'autres comptes en fonction des ressources. *Vous pouvez également utiliser une politique basée sur les ressources pour autoriser un AWS service à accéder à vos compartiments Amazon S3.*

Pour permettre un accès comptes multiples , vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une stratégie basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource se trouvent dans des AWS comptes différents, vous devez également accorder à l'entité principale l'autorisation d'accéder à la ressource. Accordez l'autorisation en attachant une stratégie basée sur les identités à l'entité. Toutefois, si une stratégie basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre stratégie basée sur l'identité n'est requise. Pour en savoir plus, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le guide de l'utilisateur IAM.

Le service Amazon S3 ne prend en charge qu'un seul type de politique basée sur les ressources, appelée stratégie de compartiment, qui est attachée à un compartiment. Cette politique définit les entités principales (comptes, utilisateurs, rôles et utilisateurs fédérés) qui peuvent effectuer des actions sur le responsable *de la facturation.*

Exemples

Pour consulter des exemples de politiques basées sur les ressources de Billing Conductor, voir Exemples de stratégies basées sur les ressources AWS Billing Conductor

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) sont des listes de bénéficiaires que vous pouvez attacher aux ressources. Elles accordent des autorisations aux comptes pour accéder aux ressources auxquelles ils sont associés. Vous pouvez associer des ACL à une ressource de compartiment Amazon *S3*.

Avec les listes de contrôle d'accès (ACL) Amazon S3, vous pouvez gérer l'accès aux ressources des *compartiments*. Chaque *compartiment* possède une liste de contrôle d'accès qui lui est attachée comme sous-ressource. Il définit les AWS comptes, les utilisateurs ou groupes d'utilisateurs IAM, ou les rôles IAM auxquels l'accès est accordé, ainsi que le type d'accès. Lorsqu'une demande est reçue pour une ressource, AWS vérifie l'ACL correspondante pour vérifier que le demandeur dispose des autorisations d'accès nécessaires.

Lorsque vous créez une ressource de *compartiment*, Amazon S3 crée une ACL par défaut qui accorde au propriétaire de la ressource le contrôle total de la ressource. Dans l'exemple de liste ACL de *compartiment* suivant, John Doe est répertorié en tant que propriétaire du *compartiment* et bénéficie d'un contrôle total sur ce *compartiment*. Une ACL peut avoir jusqu'à 100 bénéficiaires.

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://Billing Conductor.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6</ID>
    <DisplayName>john-doe</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6</ID>
        <DisplayName>john-doe</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

Le champ ID de l'ACL est l'ID utilisateur canonique du AWS compte. Pour savoir comment afficher cet identifiant dans un compte que vous possédez, consultez la section Trouver un identifiant d'utilisateur canonique pour un AWS compte.

Autorisation basée sur les tags Billing Conductor

Vous pouvez associer des balises aux ressources de Billing Conductor ou transmettre des balises dans une demande adressée à Billing Conductor. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `Billing Conductor:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Rôles IAM de Billing Conductor

Un rôle IAM est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec Billing Conductor

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

Billing Conductor prend en charge l'utilisation d'identifiants temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Rôles de service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les fonctions du service s'affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Billing Conductor soutient les rôles de service.

Choisir un rôle IAM dans Billing Conductor

Lorsque vous créez une ressource dans Billing Conductor, vous devez choisir un rôle pour permettre à Billing Conductor d'accéder à Amazon EC2 en votre nom. Si vous avez déjà créé un rôle de service ou un rôle lié à un service, Billing Conductor vous fournit une liste de rôles parmi lesquels choisir. Il est important de choisir un rôle qui permet d'accéder au démarrage et à l'arrêt des instances Amazon EC2.

AWS Billing Conductor exemples de politiques basées sur l'identité

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou à modifier les ressources de Billing Conductor. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour savoir comment créer une stratégie IAM basée sur l'identité à l'aide de ces exemples de documents de stratégie JSON, veuillez consulter Création de stratégies dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques

- Exemples de politiques basées sur l'identité de Billing Conductor

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources de Billing Conductor dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège – Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès – Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles – IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d’API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l’accès aux API protégé par MFA dans le Guide de l’utilisateur IAM.

Pour plus d’informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l’utilisateur IAM.

Exemples de politiques basées sur l'identité de Billing Conductor

Cette rubrique contient des exemples de politiques que vous pouvez associer à votre utilisateur ou groupe IAM pour contrôler l'accès aux informations et aux outils de votre compte.

Rubriques

- Octroi d'un accès complet à la console Billing Conductor
- Octroi d'un accès complet à l'API Billing Conductor
- Octroi d'un accès en lecture seule à la console Billing Conductor
- Accorder l'accès à Billing Conductor via la console de facturation
- Accorder l'accès à Billing Conductor via les rapports de AWS coûts et d'utilisation
- Accorder à Billing Conductor l'accès à la fonctionnalité d'importation d'unités organisationnelles
- Refuser à Billing et à Cost Explorer l'accès aux services et fonctionnalités qui ne prennent pas en charge les coûts pro forma

Octroi d'un accès complet à la console Billing Conductor

Pour accéder à la console Billing Conductor, vous devez disposer d'un minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources de Billing Conductor présentes dans votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs et rôles IAM) tributaires de cette politique.

Pour garantir que ces entités peuvent toujours utiliser la console Billing Conductor, associez également la politique AWS gérée suivante aux entités. Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le guide de l'utilisateur IAM :

Outre les `billingconductor:*` autorisations, elle `pricing:DescribeServices` est requise pour la création de règles de tarification et `organizations:ListAccounts` pour répertorier les comptes liés liés au compte payeur.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "billingconductor:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "pricing:DescribeServices",
            "Resource": "*"
        }
    ]
}
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Octroi d'un accès complet à l'API Billing Conductor

Dans cet exemple, vous accordez à une entité IAM un accès complet à l'API Billing Conductor.

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

```
        },
        {
            "Effect": "Allow",
            "Action": "organizations:ListAccounts",
            "Resource": "*"
        }
    ]
}
```

Octroi d'un accès en lecture seule à la console Billing Conductor

Dans cet exemple, vous accordez à une entité IAM un accès en lecture seule à la console Billing Conductor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "billingconductor:List*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:ListAccounts",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "pricing:DescribeServices",
            "Resource": "*"
        }
    ]
}
```

Accorder l'accès à Billing Conductor via la console de facturation

Dans cet exemple, les entités IAM peuvent activer et afficher les données de facturation pro forma via la page des factures de leur console de facturation.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "billing:ListBillingViews",
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        }
    ]
}
```

Accorder l'accès à Billing Conductor via les rapports de AWS coûts et d'utilisation

Dans cet exemple, les entités IAM peuvent activer et afficher les données de facturation pro forma via la page Rapports sur les coûts et l'utilisation de leur console de facturation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "billing:ListBillingViews",
                "aws-portal:ViewBilling",
                "cur:DescribeReportDefinitions"
            ],
            "Resource": "*"
        }
    ]
}
```

Accorder à Billing Conductor l'accès à la fonctionnalité d'importation d'unités organisationnelles

Dans cet exemple, les entités IAM ont un accès en lecture seule aux opérations d' AWS Organizations API spécifiques requises pour importer vos comptes d'unité organisationnelle (UO) lorsque vous créez un groupe de facturation. La fonctionnalité d'importation de l'unité d'organisation se trouve sur la console AWS Billing Conductor.

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

```
            "Effect": "Allow",
            "Action": [
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        }
    ]
}
```

Refuser à Billing et à Cost Explorer l'accès aux services et fonctionnalités qui ne prennent pas en charge les coûts pro forma

Dans cet exemple, les entités IAM se voient refuser l'accès aux services et aux fonctionnalités qui ne prennent pas en charge les coûts pro forma. Cette politique inclut une liste d'actions possibles au sein du compte de gestion et des comptes de membres individuels.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "aws-portal:ModifyAccount",
            "aws-portal:ModifyBilling",
            "aws-portal:ModifyPaymentMethods",
            "aws-portal:ViewPaymentMethods",
            "aws-portal:ViewAccount",
            "cur:GetClassic*",
            "cur:Validate*",
            "tax:List*",
            "tax:Get*",
            "tax:Put*",
            "tax:ListTaxRegistrations",
            "tax:BatchPut*",
            "tax:UpdateExemptions",
            "freetier:Get*",
            "payments:Get*",
            "payments:List*",
            "payments:Update*",
            "payments:GetPaymentInstrument",
            "payments:GetPaymentStatus",
            "purchase-orders:ListPurchaseOrders",
```

```
            "purchase-orders:ListPurchaseOrderInvoices",
            "consolidatedbilling:GetAccountBillingRole",
            "consolidatedbilling:Get*",
            "consolidatedbilling:List*",
            "invoicing:List*",
            "invoicing:Get*",
            "account:Get*",
            "account:List*",
            "account:CloseAccount",
            "account:DisableRegion",
            "account:EnableRegion",
            "account:GetContactInformation",
            "account:GetAccountInformation",
            "account:PutContactInformation",
            "billing:GetBillingPreferences",
            "billing:GetContractInformation",
            "billing:GetCredits",
            "billing:RedeemCredits",
            "billing:Update*",
            "ce:GetPreferences",
            "ce:UpdatePreferences",
            "ce:GetReservationCoverage",
            "ce:GetReservationPurchaseRecommendation",
            "ce:GetReservationUtilization",
            "ce:GetSavingsPlansCoverage",
            "ce:GetSavingsPlansPurchaseRecommendation",
            "ce:GetSavingsPlansUtilization",
            "ce:GetSavingsPlansUtilizationDetails",
            "ce:ListSavingsPlansPurchaseRecommendationGeneration",
            "ce:StartSavingsPlansPurchaseRecommendationGeneration",
            "ce:UpdateNotificationSubscription"
        ],
        "Resource": "*"
    }]
}
```

Pour plus d'informations, consultez Services AWS qui prennent en charge les coûts pro forma.

AWS politiques gérées pour AWS Billing Conductor

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour

créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSBillingConductorFullAccess

La politique AWSBillingConductorFullAccess gérée accorde un accès complet à la console et aux API AWS de Billing Conductor. Les utilisateurs peuvent répertorier, créer et supprimer des ressources AWS de Billing Conductor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "billingconductor:*",
               "organizations:ListAccounts",
               "pricing:DescribeServices",
             ]
            "Resource": "*"
        }
```

```
    ]
}
```

AWS politique gérée : AWSBillingConductorReadOnlyAccess

La politique AWSBillingConductorReadOnlyAccess gérée accorde un accès en lecture seule à la console AWS Billing Conductor et aux API. Les utilisateurs peuvent consulter et répertorier toutes les ressources AWS de Billing Conductor. Les utilisateurs ne peuvent ni créer ni supprimer de ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BillingConductorReadOnly",
            "Effect": "Allow",
            "Action": [
                "billingconductor:List*",
                "organizations:ListAccounts",
                "pricing:DescribeServices",
                "billingconductor:GetBillingGroupCostReport"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Mises à jour des politiques AWS gérées par Billing Conductor

Consultez les détails des mises à jour des politiques AWS gérées pour AWS Billing Conductor 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 des documents AWS de Billing Conductor.

Modification	Description	Date
AWSBillingConducto rReadOnlyAccess	Ajouté `GetBillin gGroupCostReport` à la `AWSBillingConducto`	8 février 2024

Modification	Description	Date
	`rReadOnlyAccess` politique.	
AWSBillingConductorFullAccess	Politique créée	29 mars 2022
AWSBillingConductorReadOnlyAccess	Politique créée	29 mars 2022
AWS Journal des modifications de Billing Conductor publié	AWS Billing Conductor a commencé à suivre les modifications apportées AWS à ses politiques gérées.	29 mars 2022

Exemples de stratégies basées sur les ressources AWS Billing Conductor

Rubriques

- Restreindre l'accès au compartiment Amazon S3 à des adresses IP spécifiques

Restreindre l'accès au compartiment Amazon S3 à des adresses IP spécifiques

L'exemple suivant accorde des autorisations à n'importe quel utilisateur pour effectuer des opérations Amazon S3 sur des objets du compartiment spécifié. Toutefois, la demande doit provenir de la plage d'adresses IP indiquée dans la condition.

La condition dans cette instruction identifie la plage 54.240.143.* d'adresses Internet Protocol version 4 (IPv4) autorisées, avec une exception : 54.240.143.188.

Le `Condition` bloc utilise les `NotIpAddress` conditions `IpAddress` et et la clé de `aws:SourceIp` condition, qui est une clé de condition AWS large. Pour plus d'informations sur ces clés de condition, consultez la section Spécification de conditions dans une politique. Les valeurs IPv4 `aws:sourceIp` font appel à la notation CIDR standard. Pour en savoir plus, consultez Opérateurs de condition d'adresse IP dans le guide de l'utilisateur IAM.

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

```
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
         "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
         "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
      }
    }
  ]
}
```

Résolution des problèmes AWS Billing Conductor d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Billing Conductor et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Billing Conductor
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources Billing Conductor

Je ne suis pas autorisé à effectuer une action dans Billing Conductor

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` IAM essaie d'utiliser la console pour consulter les détails d'un responsable *`de facturation mais ne`* dispose pas des `Billing Conductor:`*`GetWidget`* autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: Billing
 Conductor:GetWidget on resource: my-example-Billing Conductor
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *my-example-Billing Conductor* à l'aide de l'action `Billing Conductor:GetWidget`.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Billing Conductor.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Billing Conductor. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les stratégies de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources Billing Conductor

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Billing Conductor prend en charge ces fonctionnalités, consultezComment AWS Billing Conductor fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Enregistrement et surveillance dans AWS Billing Conductor

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de votre AWS compte. Plusieurs outils sont disponibles pour surveiller votre utilisation de AWS Billing Conductor.

AWS Rapports sur les coûts et l'utilisation

AWS Les rapports sur les coûts et AWS l'utilisation suivent votre utilisation et fournissent une estimation des frais associés à votre compte. Chaque rapport contient des rubriques correspondant à chaque combinaison unique de AWS produits, de type d'utilisation et d'opération que vous utilisez dans votre AWS compte. Vous pouvez personnaliser les rapports sur les AWS coûts et l'utilisation pour agréger les informations par heure ou par jour.

Pour plus d'informations sur les rapports sur les AWS coûts et l'utilisation, consultez le Guide des rapports sur les coûts et l'utilisation.

Journalisation des appels AWS Billing Conductor d'API à l'aide AWS CloudTrail

AWS Billing Conductor 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 Billing Conductor.

CloudTrail capture tous les appels d'API pour AWS Billing Conductor sous forme d'événements. Les appels capturés incluent des appels provenant de la console AWS Billing Conductor et des appels de code vers les opérations AWS de l'API Billing Conductor. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour AWS Billing Conductor. 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 à AWS Billing Conductor, 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 Billing Conductor CloudTrail événements

Cette section présente une liste complète des CloudTrail événements liés à Billing and Cost Management.

Nom de l'événement	Définition
`AssociateAccounts`	Enregistre l'association de comptes à un groupe de facturation.
`AssociatePricingRules`	Enregistre l'association des règles de tarification à un plan tarifaire.
`AutoAssociateAccount`	Enregistre l'association automatique d'un compte à un groupe de facturation.
`AutoDisassociateAccount`	Enregistre la dissociation automatique d'un compte d'un groupe de facturation lors de la prochaine période de facturation.
`BatchAssociateResourcesToCustomLineItem`	Enregistre l'association par lots de ressources dans une rubrique personnalisée en pourcentage.
`BatchDisassociateResourcesF`	Enregistre la dissociation par lots des ressources à partir d'un élément de ligne personnalisé en pourcentage.

Nom de l'événement	Définition
romCustom LineItem	
CreateBil lingGroup	Enregistre la création d'un groupe de facturation.
CreateCus tomLineItem	Enregistre la création d'un article personnalisé.
CreatePricingPlan	Enregistre la création d'un plan tarifaire.
CreatePricingRule	Enregistre la création d'une règle de tarification.
DeleteBil lingGroup	Enregistre la suppression d'un groupe de facturation.
DeleteCus tomLineItem	Enregistre la suppression d'un élément de ligne personnalisé.
DeletePricingPlan	Enregistre la suppression d'un plan tarifaire.
DeletePricingRule	Enregistre la suppression d'une règle de tarification.
Disassoci ateAccounts	Enregistre la dissociation des comptes d'un groupe de facturation.
Disassoci atePricingRules	Enregistre la dissociation des règles de tarification par rapport à un plan tarifaire.
ListAccou ntAssociations	Enregistre l'accès aux identifiants de compte dans le groupe de facturation.
ListBilli ngGroupCo stReports	Enregistre l'accès aux AWS frais réels pour le groupe de facturation.
ListBillingGroups	Enregistre l'accès aux groupes de facturation au cours d'une période de facturation.

Nom de l’événement	Définition
`ListCustomLineItems`	Enregistre l'accès aux rubriques personnalisées au cours d'une période de facturation.
`ListCustomLineItemVersions`	Enregistre l'accès aux versions d'un élément de ligne personnalisé.
`ListPricingPlans`	Enregistre l'accès aux plans tarifaires au cours d'une période de facturation.
`ListPricingPlansAssociatedWithPricingRule`	Enregistre l'accès aux plans tarifaires associés à une règle de tarification.
`ListPricingRules`	Enregistre l'accès aux règles de tarification au cours d'une période de facturation.
`ListPricingRulesAssociatedToPricingPlan`	Enregistre l'accès aux règles de tarification associées à un plan tarifaire.
`ListResourcesAssociatedToCustomLineItem`	Enregistre l'accès aux ressources associées à une rubrique personnalisée.
`ListTagsForResource`	Enregistre l'accès aux balises d'une ressource.
`TagResource`	Enregistre l'association de balises sur une ressource.
`UpdateBillingGroup`	Enregistre la mise à jour d'un groupe de facturation.

Nom de l'événement	Définition
`UpdateCustomLineItem`	Enregistre la mise à jour d'un article personnalisé.
`UpdatePricingPlan`	Enregistre la mise à jour d'un plan tarifaire.
`UpdatePricingRule`	Enregistre la mise à jour d'une règle de tarification.

AWS Informations sur le conducteur de facturation dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS Billing Conductor, 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 à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris ceux de AWS Billing Conductor, créez une trace. 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 notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions AWS de Billing Conductor sont enregistrées CloudTrail et documentées dans la référence AWS de l'API Billing Conductor.

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'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier journal de AWS Billing Conductor

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.

Rubriques

- AutoAssociateAccount
- CreateBillingGroup

AutoAssociateAccount

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


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "billingconductor.amazonaws.com"
    },
    "eventTime": "2024-02-23T00:22:08Z",
    "eventSource": "billingconductor.amazonaws.com",
```

```
    "eventName": "AutoAssociateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "billingconductor.amazonaws.com",
    "userAgent": "billingconductor.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "1v14d239-fe63-4d2b-b3cd-450905b6c33",
    "eventID": "14536982-geff-4fe8-bh18-f18jde35218d0",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "requestParameters": {
            "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666",
            "AccountIds": [
                "333333333333"
            ]
        },
        "responseElements": {
            "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666"
        }
    },
    "eventCategory": "Management"
}
```

CreateBillingGroup

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId":"111122223333",
        "accessKeyId":"ASIAIOSFODNN7EXAMPLE"
    },
    "eventTime": "2024-01-24T20:30:03Z",
    "eventSource": "billingconductor.amazonaws.com",
    "eventName": "CreateBillingGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "100.100.10.10",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
```

```
    "requestParameters": {
        "PrimaryAccountId": "444455556666",
        "ComputationPreference": {
            "PricingPlanArn": "arn:aws:billingconductor::111122223333:pricingplan/
TqeITi5Bgh"
        },
        "X-Amzn-Client-Token": "32aafb5s-e5b6-47f5-9795-3a69935e9da4",
        "AccountGrouping": {
            "LinkedAccountIds": [
                "444455556666",
                "111122223333"
            ]
        },
        "Name": "***"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666"
    },
    "requestID": "fb26ae47-3510-a833-98fe-3dc0f602gb49",
    "eventID": "3ab70d86-c63e-46fd8d-a33s-ce2970441a8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Validation de conformité pour AWS Billing Conductor

Des auditeurs tiers évaluent la sécurité et la conformité des AWS services dans le cadre de multiples programmes de AWS conformité. AWS Billing Conductor n'entre dans le champ d'application d'aucun programme de conformité d'AWS.

Pour obtenir la liste des AWS services concernés par des programmes de conformité spécifiques, voir Services AWS concernés par programme de conformité . Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour de plus amples informations, veuillez consulter Téléchargement de rapports dans AWS Artifact.

Lorsque vous utilisez AWS Billing Conductor, votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides démarrage rapide de la sécurité et de la conformité. Ces guides de déploiement traitent des considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience chez AWS Billing Conductor

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure dans AWS Billing Conductor

En tant que service géré, AWS Billing Conductor il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure,

consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Billing Conductor via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Quotas et restrictions

Le tableau suivant décrit les quotas et les restrictions au sein AWS de Billing Conductor.

Quotas

Nombre de groupes de facturation par compte payeur	5 000
Nombre de comptes par groupe de facturation	1 000
Nombre de plans tarifaires	5 000
Nombre de règles de tarification	50 000
Nombre de règles de tarification pouvant être associées à un plan tarifaire	500
Nombre de plans tarifaires pouvant être associés à une règle de tarification	1 000
Nombre d'éléments de ligne personnalisés	50 000
Nombre de valeurs source pouvant être associées à un élément de ligne personnalisé en pourcentage	100
Nombre de pourcentage personnalisé pouvant être associé à un élément de ligne personnalisé plat	100

Restrictions

Les autres restrictions du tableau suivant ne peuvent pas être augmentées.

Nombre de rapports sur les coûts et l'utilisation du groupe de facturation par groupe de facturation	10
Nom du groupe de facturation	• Doit contenir moins de 128 caractères • Ne peut pas contenir de `space` • Ne peut pas contenir de caractères spéciaux
Description du groupe de facturation	Doit contenir moins de 1 024 caractères
Nom du plan de tarification	• Doit contenir moins de 128 caractères • Ne peut pas contenir de `space` • Ne peut pas contenir de caractères spéciaux
Description du plan de tarification	Doit contenir moins de 1 024 caractères
Nom de l'élément de ligne personnalisé	• Doit contenir moins de 128 caractères • Ne peut pas contenir de `space` • Ne peut pas contenir de caractères spéciaux

Historique du document

Le tableau suivant décrit la documentation de cette version de AWS Billing Conductor.

Modification	Description	Date
Documentation mise à jour	Mise à jour du What is AWS Billing Conductor ? sujet.	7 mars 2024
Documentation mise à jour pour les politiques AWS gérées	Ajouté `GetBillingGroupCostReport` à la `AWSBillingConductorReadOnlyAccess` politique. Voir les politiques AWS gérées pour AWS Billing Conductor.	8 février 2024
Documentation ajoutée pour le résumé des marges	Vous pouvez consulter le détail de vos marges par Service AWS groupe de facturation. Consultez la section Analyse de vos marges par groupe de facturation.	14 décembre 2023
Ajout de documentation sur les articles personnalisés	Vous pouvez appliquer un élément personnalisé à un compte associé spécifique de votre groupe de facturation. Consultez la section Création de rubriques personnalisées par groupe de facturation.	4 décembre 2023
Ajout de documentation sur le compte principal	Découvrez comment le choix d'un compte principal peut affecter vos coûts pro forma pour vos groupes de facturati	26 octobre 2023

	on. Consultez Comprendre l'importance de la date d'adhésion au compte principal .	
Ajout de la prise en charge des filtres d'articles personnalisés	Vous pouvez désormais définir des filtres de rubriques pour vos rubriques personnalisées. Pour plus d'informations, consultez la section Création d'une rubrique personnalisée avec un pourcentage de frais.	5 septembre 2023
Ajout de documentation sur les coûts pro forma	Consultez les rubriques suivantes : • Réalisation d'une analyse ad hoc sur les coûts pro forma dans AWS Cost Explorer • Services AWS qui prennent en charge les coûts pro forma • Exemple de politique IAM : refuser l'accès aux coûts pro forma	22 août 2023
Ajout du support pour l'association automatique de comptes	Vous pouvez désormais activer un groupe de facturation pour l'association automatique de comptes. Pour plus d'informations, consultez Création de groupes de facturation, configurations de tarification et articles personnalisés.	26 juillet 2023

Ajout du support de téléchargement CSV	Vous pouvez désormais télécharger un fichier CSV pour le tableau d'analyse des marges de votre groupe de facturation. Pour plus d'informations, consultez la section Analyse de vos marges par groupe de facturation.	6 juin 2023
Première version	Publication initiale du guide de l'utilisateur de AWS Billing Conductor et de la référence de l'API.	16 mars 2022

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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.