aws

Guide de l’utilisateur

Profileur des coûts d'application

Profileur des coûts d'application: Guide de l’utilisateur

Table of Contents

AWS Application Cost Profiler ne sera plus disponible d'ici le 30 septembre 2024 et n'accepte plus de nouveaux clients.

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.

Présentation d'AWSApplication Cost Profiler ?

AWSApplication Cost Profiler vous aide à séparer votreAWSfacturation et coûts par les locataires de votre service. UNlocatairepeut être un utilisateur, un groupe d'utilisateurs ou un projet.

UNressourceest une entité avec laquelle les utilisateurs peuvent travailler dansAWS, telle qu'une instance Amazon Elastic Compute Cloud (Amazon EC2). Assurez-vous que vous pouvez identifier l'utilisation de vos ressources par le locataire que vous choisissez.

TypiqueAWSL'utilisation des ressources inclut des services partagés qui prennent en charge plusieurs locataires au sein de votre organisation. Certaines ressources utilisent des dimensions temporelles. Pour obtenir des informations de coût et de facturation par locataire plutôt que par utilisation horaire de la ressource, vous pouvez intégrer vos ressources à Application Cost Profiler. Avec cette approche granulaire, vous pouvez comprendre commentAWSles ressources sont consommées dans une solution logicielle partagée.

Les ressources suivantes pouvant utiliser des dimensions temporelles ou une utilisation horaire sont activées pour Application Cost Profiler :

- Instances Amazon EC2 (instances à la demande et ponctuelles uniquement)
- Files d'attente Amazon Simple Queue Service (Amazon SQS)
- Rubriques Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB lit et écrit

> **Note**
>
> L'utilisation d'Amazon SQS, Amazon SNS et DynamoDB n'est pas facturée par le temps, contrairement à la plupart des ressources. Dans leur cas, l'utilisation pendant une heure (par exemple, un certain nombre de lectures et d'écritures dans DynamoDB) est classée en fonction du pourcentage de l'heure que vous allouez à différents locataires, quel que soit le moment où les lectures ou les écritures ont eu lieu pendant l'heure.

Vous intégrez vos services à Application Cost Profiler en trois étapes :

1. Activer et configurer un rapport— Cette étape définit à quoi ressemble votre sortie finale.

2. Envoyer des données d'utilisation des locataires à Application Cost Profiler— Cette étape nécessite du code dans votre service pour créer des données d'utilisation associant les locataires au moment où ils utilisent vos ressources, puis envoyez ces données d'utilisation à Application Cost Profiler.
3. Réduction de rapports— Application Cost Profiler fournit des rapports à la cadence que vous avez spécifiée dans la configuration de votre rapport. Les rapports indiquent le coût associé à l'utilisation de chaque locataire, ce qui vous donne une vue granulaire de votre facturation.

Pour de plus amples informations sur ces étapes, consultezPremiers pas.

Commencer à utiliser Application Cost Profiler

AWS Application Cost Profiler vous aide à obtenir des informations sur les coûts de vos AWS ressources en signalant l'utilisation des ressources par locataire, plutôt que pour la ressource dans son ensemble. Un locataire peut être un utilisateur, un groupe d'utilisateurs ou un projet. Assurez-vous de pouvoir identifier l'utilisation de vos ressources par le locataire que vous choisissez. Pour obtenir des rapports sur les coûts relatifs à l'utilisation des locataires, vous configurez un rapport et envoyez les données d'utilisation à Application Cost Profiler. Cette section décrit les conditions préalables que vous devez remplir avant d'utiliser Application Cost Profiler.

Rubriques

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

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

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

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l‘utilisateur racine a accès à l‘ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l‘utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, voir Activer un MFA périphérique virtuel pour votre utilisateur Compte AWS root (console) dans le guide de IAM l'utilisateur.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu‘utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URLidentifiant envoyé à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAMIdentity Center, consultez la section Connexion au portail AWS d'accès dans le guide de Connexion à AWS l'utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme à la meilleure pratique consistant à appliquer les autorisations du moindre privilège.

   Pour obtenir des instructions, consultez Création d’un ensemble d’autorisations dans le Guide de l’utilisateur AWS IAM Identity Center .
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l’utilisateur AWS IAM Identity Center .

Octroi d’un accès par programmation

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l’une des options suivantes.

Quel utilisateur a besoin d’un accès programmatique ?	Pour	Par
Identité de la main-d’œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées	Suivez les instructions de l’interface que vous souhaitez utiliser.

Quel utilisateur a besoin d’un accès programmatique ?	Pour	Par
	au AWS CLI AWS SDKs, ou AWS APIs.	• Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour AWS SDKs, outils, et AWS APIs, voir Authentification IAM Identity Center dans le guide de référence AWS SDKs et Tools.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec les AWS ressources du Guide de IAM l'utilisateur.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Authentification à l'aide des informations IAM d'identification utilisateur dans le Guide de AWS Command Line Interface l'utilisateur. • Pour les outils AWS SDKs et, voir Authentifier à l'aide d'informations d'identification à long terme dans le guide de référence des outils AWS SDKs et. • Pour AWS APIs, voir Gestion des clés d'accès pour IAM les utilisateurs dans le Guide de IAM l'utilisateur.

Conditions préalables spécifiques à Application Cost Profiler

Avant de commencer à utiliser Application Cost Profiler, vous devez remplir les conditions préalables suivantes :

- Activer Cost Explorer

  Activez AWS Cost Explorer pour votre AWS compte. La création d'un compte auprès de Cost Explorer peut prendre jusqu'à 24 heures. Vous devez terminer la configuration de Cost Explorer avant qu'Application Cost Profiler puisse générer vos rapports quotidiens et mensuels.

Pour plus d'informations, consultez la section Activation de Cost Explorer dans le guide de AWS Billing and Cost Management l'utilisateur.

- Création de compartiments S3

  Créez au moins deux compartiments Amazon Simple Storage Service (Amazon S3). Application Cost Profiler utilise un compartiment S3 pour vous fournir des rapports. Vous utilisez l'autre compartiment S3 pour télécharger les données d'utilisation dans Application Cost Profiler. Généralement, vous n'avez besoin que d'un seul compartiment S3 pour télécharger les données d'utilisation. Toutefois, vous souhaiterez peut-être disposer de plusieurs compartiments S3 afin de pouvoir continuer à utiliser différents services dans des compartiments S3 distincts dotés d'autorisations différentes, si cela est nécessaire pour votre sécurité. Vous devez autoriser Application Cost Profiler à accéder à ces compartiments S3.

  Pour plus d'informations sur la configuration des compartiments Amazon S3 pour Application Cost Profiler, consultez. Configuration des compartiments Amazon S3 pour Application Cost Profiler

- Activer les balises

  Pour signaler l'utilisation par balise plutôt que par ressource, vous devez activer ces balises dans la AWS Billing and Cost Management console.

  Pour plus d'informations sur l'activation des balises AWS générées, voir Activation des balises de répartition des coûts AWS générées dans le guide de l'AWS Billing and Cost Management utilisateur. Pour plus d'informations sur l'activation des balises définies par l'utilisateur, voir Activation des balises de répartition des coûts définies par l'utilisateur dans le guide de l'AWS Billing and Cost Management utilisateur.

Étapes suivantes

Après avoir rempli ces prérequis, vous pouvez :

- Configurez votre rapport et envoyez les données d'utilisation à Application Cost Profiler. Pour de plus amples informations, veuillez consulter Création de votre rapport.
- Obtenez et analysez les rapports que vous avez générés. Pour de plus amples informations, veuillez consulter Utilisation des rapports Application Cost Profiler.

Configuration des compartiments Amazon S3 pour Application Cost Profiler

Pour envoyer des données d'utilisation et recevoir des rapports depuisAWSApplication Cost Profiler, vous devez disposer d'au moins un compartiment Amazon Simple Storage Service (Amazon S3) dans votre compartimentCompte AWSpour stocker les données et un compartiment S3 pour recevoir vos rapports.

> **Note**
>
> Pour les utilisateurs deAWS Organizations, les compartiments Amazon S3 peuvent se trouver dans le compte de gestion ou dans des comptes membres individuels. Les données des compartiments S3 appartenant au compte de gestion peuvent être utilisées pour générer des rapports pour l'ensemble de l'organisation. Dans les comptes de membres individuels, les données des compartiments S3 ne peuvent être utilisées que pour générer des rapports pour ce compte membre.

Les compartiments S3 que vous créez appartiennent auCompte AWSdans lequel vous les créez. Les godets S3 sont facturés aux tarifs Amazon S3 standard. Pour plus d'informations sur la façon de créer un compartiment Amazon S3, consultezCréer un compartimentdans leManuel de l'utilisateur d'Amazon Simple Storage Service.

Pour que Application Cost Profiler puisse utiliser les compartiments S3, vous devez attacher une stratégie aux compartiments qui autorise Application Cost Profiler à lire et/ou écrire dans celui-ci. Si vous modifiez la stratégie après la configuration de vos rapports, vous pouvez empêcher Application Cost Profiler de pouvoir lire vos données d'utilisation ou fournir vos rapports.

Les rubriques suivantes expliquent comment configurer des autorisations sur vos compartiments Amazon S3 après les avoir créés. Outre la possibilité de lire et d'écrire des objets, si vous avez chiffré les compartiments, Application Cost Profiler doit avoir accès auAWS Key Management Service(AWS KMS) pour chaque seau.

Rubriques

Donner à Application Cost Profiler l'accès à votre compartiment S3 de livraison de rapports

Le compartiment S3 que vous configurez pour que Application Cost Profiler fournisse vos rapports doit être associé à une stratégie permettant à Application Cost Profiler de créer les objets de rapport. En outre, le compartiment S3 doit être configuré pour activer le chiffrement.

> **Note**
>
> Lorsque vous créez votre compartiment, vous devez choisir de le chiffrer. Vous pouvez choisir de chiffrer votre compartiment avec des clés gérées par Amazon S3 (SSE-S3) ou avec votre propre clé gérée parAWS KMS(SE-KMS). Si vous avez déjà créé votre compartiment sans chiffrement, vous devez modifier votre compartiment pour ajouter le chiffrement.

Pour donner à Application Cost Profiler l'accès à votre compartiment S3 de livraison de rapports

1. Accédez à laConsole Amazon S3et connectez-vous.
2. Tâche de sélectionCompartimentsdans la barre de navigation de gauche, puis choisissez votre compartiment dans la liste.
3. Cliquez sur l'ongletAutorisations, puis à côté deStratégie de compartiment, choisissezModifier.
4. DansStratégie, insérez la stratégie suivante. Remplacez*<bucket_name>*par le nom de votre compartiment, et*<Compte AWS>*par l'ID de votreCompte AWS.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
          "Action":[
            "s3:PutObject*",
            "s3:GetEncryptionConfiguration"
          ],
          "Resource": [
            "arn:aws:s3:::<bucket-name>",
```

```
            "arn:aws:s3:::<bucket-name>/*"
          ],
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<Compte AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-
east-1:<Compte AWS>:*"
            }
          }
        }
      ]
    }
```

Dans cette politique, vous indiquez le principal du service Application Cost Profiler (`application-cost-profiler.amazonaws.com`) pour distribuer les rapports dans le compartiment spécifié. Elle le fait en votre nom et inclut un en-tête avec votreCompte AWSet un ARN spécifique à votre compartiment de livraison de rapports. Pour s'assurer que Application Cost Profiler n'accède à votre compartiment que lorsqu'il agit en votre nom, le`Condition`vérifie la présence de ces en-têtes.

5. ChoisissezEnregistrez les modificationspour enregistrer votre stratégie, attachée à votre compartiment.

   Si vous avez créé votre compartiment à l'aide du chiffrement SSE-S3, c'est terminé. Si vous avez utilisé le chiffrement SSE-KMS, les étapes suivantes sont nécessaires pour donner accès à Application Cost Profiler à votre compartiment.

6. (Facultatif) Choisissez laPropriétéspour votre compartiment, et sousChiffrement par, sélectionnez l'Amazon Resource Name (ARN) pour votreAWS KMSclé. Cette action affiche leAWS Key Management Serviceet affiche votre clé.

7. (Facultatif) Ajoutez la stratégie pour donner accès à Application Cost Profiler auAWS KMSclé. Pour obtenir des instructions sur l'ajout de cette politique, consultezDonner accès à Application Cost Profiler aux compartiments S3 chiffrés SSE-KMS.

Donner à Application Cost Profiler l'accès à votre compartiment S3 de données d'utilisation

Le compartiment S3 que vous configurez pour Application Cost Profiler pour lire vos données d'utilisation doit être associé à une stratégie pour permettre à Application Cost Profiler de lire les objets de données d'utilisation.

> **Note**
>
> En donnant à Application Cost Profiler l'accès à vos données d'utilisation, vous acceptez que nous puissions copier temporairement ces objets de données d'utilisation vers l'Est des États-Unis (Virginie du Nord)Région AWSlors du traitement des rapports. Ces objets de données seront conservés dans la région US East (N. Virginia) jusqu'à ce que la génération des rapports mensuels soit terminée.

Pour donner à Application Cost Profiler l'accès à votre compartiment S3 de données d'utilisation

1. Accédez à laConsole Amazon S3et connectez-vous.
2. Tâche de sélectionCompartimentsdans la barre de navigation de gauche, puis choisissez votre compartiment dans la liste.
3. Cliquez sur l'ongletAutorisations, puis à côté deStratégie de compartiment, choisissezModifier.
4. DansStratégie, insérez la stratégie suivante. Remplacez*<bucket-name>*par le nom de votre compartiment, et*<Compte AWS>*par l'ID de votreCompte AWS.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
          "Action":[
            "s3:GetObject*"
          ],
          "Resource": [
            "arn:aws:s3:::<bucket-name>",
            "arn:aws:s3:::<bucket-name>/*"
```

```
          ],
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<Compte AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-
east-1:<Compte AWS>:*"
            }
          }
        }
      ]
    }
```

Dans cette politique, vous indiquez le principal du service Application Cost Profiler (`application-cost-profiler.amazonaws.com`) pour extraire des données d'un compartiment spécifié. Elle le fait en votre nom et inclut un en-tête avec votreCompte AWSet un ARN spécifique à votre compartiment d'utilisation. Pour s'assurer que Application Cost Profiler n'accède à votre compartiment que lorsqu'il agit en votre nom, le`Condition`vérifie la présence de ces en-têtes.

5. ChoisissezEnregistrez les modificationspour enregistrer votre stratégie, attachée à votre compartiment.

Si votre compartiment est chiffré avecAWS KMSclés gérées, vous devez alors donner à Application Cost Profiler l'accès à votre compartiment en suivant la procédure de la section suivante.

Donner accès à Application Cost Profiler aux compartiments S3 chiffrés SSE-KMS

Si vous chiffrez les compartiments S3 que vous configurez pour Application Cost Profiler (requis pour les compartiments de rapport) avec des clés stockées dansAWS KMS(SSE-KMS), vous devez également accorder des autorisations à Application Cost Profiler pour les déchiffrer. Pour ce faire, vous donnez accès auAWS KMSclés utilisées pour chiffrer les données.

> **Note**
>
> Si votre compartiment est chiffré avec des clés gérées Amazon S3, vous n'avez pas besoin de terminer cette procédure.

Pour donner accès à Application Cost Profiler àAWS KMSpour compartiments S3 chiffrés SSE-KMS

1. Accédez à laAWS KMSconsoleet connectez-vous.
2. Tâche de sélectionClés gérées par le clientdans la navigation de gauche, puis choisissez la clé qui est utilisée pour chiffrer votre compartiment dans la liste.
3. Tâche de sélectionBasculer vers la vue de stratégie d', puis choisissezModifier.
4. DansStratégie, insérez la déclaration de politique suivante.

```
  {
    "Effect": "Allow",
    "Principal": {
        "Service": "application-cost-profiler.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<Compte AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-
east-1:<Compte AWS>:*"
            }
  }
```

5. ChoisissezEnregistrez les modificationspour enregistrer votre stratégie, attachée à votre clé.
6. Répétez cette opération pour chaque clé qui chiffre un compartiment S3 auquel Application Cost Profiler doit accéder.

> **Note**
>
> Les données sont copiées depuis votre compartiment S3 lors de leur importation dans des compartiments gérés Application Cost Profiler (chiffrés). Si vous révoquez l'accès aux clés, Application Cost Profiler ne peut pas récupérer de nouveaux objets du compartiment.

Toutefois, toutes les données déjà importées peuvent toujours être utilisées pour générer des rapports.

Création de votre rapport

Une fois les conditions requises remplies, vous êtes prêt à configurer le rapport correspondant à votre utilisationCompte AWS et à envoyer vos données d'utilisation àAWS Application Cost Profiler. Cette section explique comment configurer le rapport et comment envoyer les données d'utilisation à Application Cost Profiler.

Application Cost st Prost st st st st st Prost st st

La procédure suivante montre comment configurer le rapport que vous souhaitez générer en fonction de votre date d'utilisation. Vous configurez des détails tels que la fréquence à laquelle le rapport est généré.

> **Note**
>
> Si vousCompte AWS faites partie d'uneAWS organisation, vous pouvez configurer le rapport à l'aide du compte de gestion ou d'un compte de membre individuel. Les rapports configurés pour des comptes individuels contiennent uniquement des données relatives à ce compte. Les rapports configurés à l'aide du compte de gestion peuvent inclure des données pour l'ensemble de l'organisation.
> Le compartiment Amazon S3 utilisé pour la sortie du rapport doit appartenir au compte qui crée la configuration du rapport.

Pour configurer votre rapport Application Cost Profiler

1. Ouvrez un navigateur Web et connectez-vous à la console Application Cost Profiler.
2. Choisissez Commencer maintenant pour configurer ou modifier un rapport.
3. Entrez un nom de rapport et une description pour votre rapport.
4. Entrez le nom de votre compartiment S3 dans le champ Entrez le nom du compartiment S3 et entrez le préfixe S3 dans le champ Entrez le préfixe S3. Pour plus d'informations sur la création de compartiments S3 et l'octroi d'autorisations à Application Cost Profiler, consultezConfiguration des compartiments Amazon S3 pour Application Cost Profiler.
5. Sélectionnez les options que vous souhaitez attribuer à votre rapport :

- Fréquence : choisissez si le rapport est généré selon une cadence quotidienne ou mensuelle, ou les deux.
- Format de sortie du rapport : choisissez le type de fichier à créer dans votre compartiment Amazon S3. Si vous choisissez CSV, Application Cost Profiler crée un fichier texte de valeurs séparées par des virgules avec compression gzip pour les rapports. Si vous choisissez Parquet, un fichier Parquet est généré pour les rapports.

6. Choisissez Configurer pour enregistrer la configuration de votre rapport.

> **Note**
>
> Vous pouvez également utiliser l'APIAWS Application Cost Profiler pour configurer les rapports.

Vérifiez les paramètres du rapport en choisissant Commencer maintenant pour afficher la configuration actuelle du rapport.

> **Note**
>
> Vous ne pouvez configurer qu'un seul rapport. Revenez à la page de configuration pour modifier votre rapport existant.

Une fois que vous avez configuré votre rapport, l'ingestion de données est activée. Vous pouvez intégrer vos services à Application Cost Profiler afin de fournir des données d'utilisation pour vos ressources.

Création de rapports sur les données d'utilisation des locataires à partir de vos services

Après avoir configuré le rapport, vous êtes prêt à envoyer les données d'utilisation des locataires à partir des ressources ou des services de votre compte. Vous devez informer Application Cost Profiler lorsque votre ressource est utilisée pour un locataire spécifique. Par exemple, si votre service accepte des appels d'API provenant de différents locataires, vous enregistrez une heure de début et de fin pour chaque client lorsque vous commencez et terminez un appel d'API provenant de ce client.

Application Cost Profiler utilise ces données pour générer des rapports sur le coût de votre service, en fonction du temps consacré au travail par chaque locataire.

Pour communiquer les données d'utilisation de l'application Cost Prost Prost st Prost Prost Prost st Prost st Prost st Prost

- Préparez les données d'utilisation des ressources : créez des tables qui décrivent quand une ressource est utilisée pour un locataire spécifique.
- Charger les données d'utilisation : chargez les tables dans un compartiment Amazon S3 auquel vous avez autorisé Application Cost Profiler à accéder.
- Importer les données d'utilisation : appelez l'opération d'`ImportApplicationUsage`API pour indiquer à Application Cost Profiler que les données sont prêtes à être traitées.

Les sections suivantes décrivent chacune de ces étapes plus en détail.

Rubriques

Étape 1 : Préparation de vos données d'utilisation des ressources

Lorsqu'une ressource est utilisée dans votre service, vous pouvez suivre le locataire qui l'utilise. Enregistrez ces données dans un tableau que vous pourrez charger ultérieurement pour qu'Application Cost Profiler puisse les importer. Chaque ligne du tableau décrit une ressource, le locataire qui utilise la ressource, ainsi que les heures de début et de fin de cette utilisation. L'instance Amazon Elastic Compute Cloud (Amazon EC2) qui est utilisée est un exemple de ressource.

Cette étape nécessite que vous intégriez du code à votre service pour générer les informations correctes sur l'utilisation.

Les champs figurant dans un tableau d'utilisation des ressources sont répertoriés dans le tableau suivant.

Champ	Description
ApplicationId	Identifie l'application ou le produit de votre système qui est utilisé. Définit l'étendue des métadonnées du client.
TenantId	Un identifiant dans votre système pour le locataire qui consomme la ressource spécifiée. Le profileur des coûts des applications s'agrège à ce niveau dans le ApplicationId.
TenantDesc	(Facultatif) Données supplémentaires sur le locataire pour vos propres rapports supplémentaires.
UsageAccountId	Le compte dans lequel la ressource s'exécute (important pour les comptes faisant partie d'une organisation).
StartTime	Horodatage (en millisecondes et microsecondes) d'Epoch, en UTC. Indique l'heure de début de la période d'utilisation par le locataire spécifié.
EndTime	Horodatage (en millisecondes et microsecondes) d'Epoch, en UTC. Indique l'heure de fin de la période d'utilisation par le locataire spécifié.
ResourceId	Amazon Resource Name (ARN) de la ressource utilisée.
Name (Nom)	(Facultatif) Au lieu de spécifier une ResourceId, vous pouvez spécifier une balise de ressource Name pour attribuer des coûts à un ensemble de ressources (le champ doit inclure la valeur que vous souhaitez utiliser pour la balise Name). Les balises de ressources sont

Champ	Description
	activées dans le cadre de votre rapport d'utilisation et de coût. Pour plus d'informations sur les balises de ressources, reportez-vous à la section Détails des balises de ressources dans le Guide de l'utilisateur du rapport sur les coûts et l'utilisation.

La sortie doit se trouver dans un fichier de valeurs séparées par des virgules (.csv) qui inclut une ligne d'en-tête, comme le montre l'exemple suivant.

```
ApplicationId,TenantId,TenantDesc,UsageAccountId,StartTime,EndTime,ResourceId
MyApp,Tenant1,,123456789012,1613681437032.9001,1613681437041.5312,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681245531.4426,1613681245551.1323,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant1,,123456789012,1613681904815.3381,1613681904930.0972,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681904765.1956,1613681904946.574,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
```

Enregistrez les données sous forme de fichier, avec une extension .csv (ou .csv.gzip si elles sont compressées avec gzip). Lorsque vous chargez ces données dans Application Cost Profiler, chaque tranche de temps est attribuée au locataire associé. Dans cet exemple, le rapport inclut la tranche horaire du coût de l'instance Amazon EC2 pour ce locataire. Pour les instances Amazon EC2 uniquement, les tranches qui ne sont pas associées à un locataire spécifique sont ajoutées à un locataire non attribué. Les tranches de temps qui se chevauchent sont comptées plusieurs fois. Il est de votre responsabilité de vous assurer que les données de votre tableau d'utilisation sont exactes.

> **Note**
>
> Votre fichier doit représenter une heure. Si une ressource est utilisée pendant plusieurs heures, mettez fin à l'utilisation à cette heure et créez un nouvel enregistrement dans le fichier suivant qui commence à la même heure.

Vous devez soumettre un seul fichier contenant les données d'une heure complète. Si plusieurs fichiers sont soumis pour les données de la même heure, Application Cost Profiler ne prend en compte que les données du dernier fichier.

Par exemple, le tableau suivant montre comment Application Cost Profiler calcule l'utilisation pour trois locataires, sur une heure (3 600 000 millisecondes), en fonction des tranches de temps fournies.

Locataire	Tranches de temps fournies	Pourcentage calculé du coût horaire
Locataire 1	1 200 000 ms	33,34 %
Locataire 2	600 000 ms	16,66 %
<unattributed>		50,00 %

Dans cet exemple, le tiers de l'heure est attribué à Tenant1 et le sixième à Tenant2. La demi-heure restante (1 800 000 ms) n'est attribuée à aucun des clients, soit 50 % de l'heure.

Actuellement, les ressources suivantes sont activées pour Application Cost Profiler :

- Instances Amazon EC2 (à la demande et instances ponctuelles uniquement)
- Fonctions Lambda (si vous envoyez des données pour une fonction Lambda, vous devez envoyer l'ARN de la ressource non qualifiée sous la forme`ResourceId`.)
- Amazon Elastic Container Service (Amazon ECS)
- Files d'attente Amazon Simple Queue Service (Amazon SQS)
- Rubriques Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB lit et écrit

Note

L'utilisation d'Amazon SQS, Amazon SNS et DynamoDB n'est pas facturée en fonction du temps, contrairement à la plupart des ressources. Dans leur cas, l'utilisation pendant une heure (par exemple, un certain nombre de lectures et d'écritures dans DynamoDB) est

classée en fonction du pourcentage d'heure que vous allouez aux différents locataires, quel que soit le moment où les lectures ou écritures ont eu lieu pendant l'heure.

Étape 2 : Chargement de l'utilisation de vos ressources

Une fois que vous disposez d'un fichier d'utilisation par locataire, chargez votre fichier de données sur Amazon S3 et assurez-vous que Application Cost Profiler est autorisé à y accéder.

Pour plus d'informations sur la création d'un compartiment S3, consultezConditions préalables spécifiques à Application Cost Profiler.

Vous devez vous assurer que Application Cost Profiler a accès à votre compartiment S3. Cela ne doit être fait qu'une seule fois par compartiment S3 (vous pouvez réutiliser le même compartiment pour télécharger plusieurs fichiers d'utilisation). Pour plus d'informations sur l'accès au compartiment, consultezDonner à Application Cost Profiler l'accès à votre compartiment S3 de données d'utilisation. Si le compartiment est chiffré, consultezDonner accès à Application Cost Profiler aux compartiments S3 chiffrés SSE-KMS.

> **Note**
>
> Il n'est pas nécessaire de chiffrer les compartiments S3 que vous utilisez pour les données d'utilisation.

Importez vos données dans le compartiment S3 sous forme de fichier, avec une extension .csv (ou .csv.gzip s'il est compressé avec gzip), toutes les heures. Après avoir chargé un nouveau fichier, vous devez informer Application Cost Profiler que vous l'avez chargé afin que le fichier puisse être importé dans votre rapport.

> **Note**
>
> En donnant à Application Cost Profiler l'accès à vos données d'utilisation, vous acceptez que nous puissions copier temporairement ces objets de données d'utilisation vers l'est des États-Unis (Virginie du Nord)Région AWS lors du traitement des rapports. Ces objets de données seront conservés dans la région USA Est (N. Virginia) jusqu'à la fin de la génération du rapport mensuel.

Étape 3 : Importation des données d'utilisation dans Application Cost Profiler

Après avoir chargé les données d'utilisation dans un compartiment Amazon S3 auquel Application Cost Profiler a accès, informez Application Cost Profiler que les données existent et importez-les dans votre rapport final. Pour ce faire, utilisez l'`ImportApplicationUsage`opération de l'API Application Cost Profiler.

Pour plus d'informations sur l'APIAWS Application Cost Profiler, y compris son`ImportApplicationUsage` fonctionnement, consultez la référence de l'APIAWS Application Cost Profiler.

L'exemple suivant de indique comment appeler`ImportApplicationUsage`. Remplacez le *`texte saisi entre crochets`* par les valeurs de votre compartiment S3 et de l'objet chargé.

```
POST /ImportApplicationUsage HTTP/1.1
Content-type: application/json

{
    "sourceS3Location" : {
        "bucket": "<bucket-name>",
        "key": "<object-key>",
        "region": "<region-id>"
    }
}
```

> **Note**
>
> L`eregion` paramètre n'est requis que si votre compartiment se trouve dans unRégion AWS compartiment désactivé par défaut. Pour plus d'informations, consultez Gestion de Régions AWS dans le Références générales AWS.

Application Cost Profiler génère un nouveau rapport à la fréquence que vous avez demandée lors de la configuration de votre rapport, en utilisant les données que vous avez importées`ImportApplicationUsage`.

Après avoir configuré votre rapport et importé automatiquement vos données d'utilisation dans Application Cost Profiler, vous êtes prêt à consulter les rapports générés. Pour plus d'informations sur les rapports, consultezUtilisation des rapports Application Cost Profiler.

Utilisation des rapports Application Cost Profiler

Une fois que vous avez intégré vos données d'utilisation àAWSApplication Cost Profiler et envoie les données toutes les heures, Application Cost Profiler génère automatiquement votre rapport.

Les rapports sont générés quotidiennement ou mensuellement, en fonction de l'option que vous avez sélectionnée lorsqueconfiguration de votre rapport. Les rapports sont livrés dans le compartiment Amazon Simple Storage Service (Amazon S3) que vous avez sélectionné lors de la configuration du rapport.

Les rapports quotidiens générés le premier jour du mois contiennent les données du mois précédent.

Données disponibles dans un rapport Application Cost Profiler

Les colonnes créées dans un rapport d'utilisation figurent dans le tableau suivant.

Nom de la colonne	Description
PayerAccountId	L'ID du compte de gestion dans une organisation ou l'ID de compte si le compte ne fait pas partie deAWS Organizations.
UsageAccountId	ID de compte du compte utilisé.
LineItemType	Type de l'enregistrement. Toujours `Usage`.
Heure de début d'utilisation	Horodatage (en millisecondes) depuis Epoch, en UTC. Indique l'heure de début de la période d'utilisation par le locataire spécifié.
Heure de fin d'utilisation	Horodatage (en millisecondes) depuis Epoch, en UTC. Indique l'heure de fin de la période d'utilisation par le locataire spécifié.
Identifiant d'application	LeApplicationIdspécifié dans les données d'utilisation envoyées à Application Cost Profiler.

Nom de la colonne	Description
Identificateur Tentaire	LeID de locatairespécifié dans les données d'utilisation envoyées à Application Cost Profiler. Les données sans enregistrement dans les données d'utilisation sont collectées dans`unattributed` .
Description du locataire	Le`TenantDesc` spécifié dans les données d'utilisation envoyées à Application Cost Profiler.
ProductCode	LeAWSproduit facturé (par exemple,`AmazonEC2`).
UsageType	Le type d'utilisation facturé (par exemple,`BoxUsage:c5.large`).
Opération	L'opération facturée (par exemple,`RunInstances`).
ID de ressource	ID de ressource ou Amazon Resource Name (ARN) de la ressource facturée.
Facteur d'échelle	Si une ressource est surallouée pendant une heure, par exemple, les données d'utilisation déclarées sont égales à 2 heures au lieu d'une heure, un facteur d'échelle est appliqué pour que le total soit égal au montant facturé réel (dans ce cas, 0,5). Cette colonne indique le facteur d'échelle utilisé pour la ressource spécifique pour cette heure. Le facteur d'échelle est toujours supérieur à zéro (0) et inférieur ou égal à 1.
Attribution des locataires en pourcentage	Pourcentage de l'utilisation attribuée au locataire spécifié (entre zéro (0) et 1).

Nom de la colonne	Description
UsageAmount	Quantité d'utilisation attribuée au locataire spécifié.
CurrencyCode	La devise dans laquelle se trouvent le taux et le coût (par exemple,USD).
Rate (Fréquence)	Le taux de facturation pour l'utilisation, par unité.
Coût du locataire	Le coût total de cette ressource pour le locataire spécifié.
Région	LeAWSRégion de la ressource.
Nom	Si vous avez créé des balises de ressource s pour vos ressources dans le rapport Cost and Usage, ou via les données d'utilisation des ressources, leNomest illustré ici. Pour en savoir plus sur les balises de ressource, consultez Détails des balises de ressourcedans leGuide de l'utilisateur du rapport d'utilisation et de coût.

Voici un exemple de rapport de sortie d'une ressource pendant deux heures.

```
PayerAccountId,UsageAccountId,LineItemType,UsageStartTime,UsageEndTime,ApplicationIdentifier,Te
123456789012,123456789012,Usage,2021-02-01T00:00:00.000Z,2021-02-01T00:30:00.000Z,Canary,unattr
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T00:30:00.000Z,2021-02-01T01:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
```

Dans cet exemple, la première heure est allouée à`Tenant1`pendant la moitié du temps. Il reste une demi-heure comme`unattributed`. Au cours de la deuxième heure, quatre locataires se voient attribuer l'heure complète. Dans ce cas, le facteur d'échelle les redimensionne tous de 0,25, et ils sont tous alloués au quart de l'heure. Vous pouvez voir le coût final dans le`TenantCost`column.

AWSQuotas et points de terminaison Application Cost Profiler

Votre compte AWS dispose de quotas par défaut, anciennement appelés limites, pour chaque service AWS. Sauf indication contraire, chaque quota estAWSSpécifique à une région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Les tableaux suivants répertorient les quotas de service par compte et leAWSPoints de terminaison de région pour Application Cost Profiler.

Quotas de Service

Ressource	Valeur par défaut	Description
Taux de`PutReportDefinition` demandes	5	Nombre maximal de`PutReportDefinition` Demandes toutes les secondes par compte
Taux de`UpdateReportDefinition` demandes	5	Nombre maximal de`UpdateReportDefinition` Demandes toutes les secondes par compte
Taux de`GetReportDefinition` demandes	5	Nombre maximal de`GetReportDefinition` Demandes toutes les secondes par compte
Taux de`DeleteReportDefinition` demandes	5	Nombre maximal de`DeleteReportDefinition` Demandes toutes les secondes par compte
Taux de`ListReportDefinitions` demandes	5	Nombre maximal de`ListReportDefiniti`

Ressource	Valeur par défaut	Description
		ons Demandes toutes les secondes par compte
Taux deImportApplicationUsage demandes	5	Nombre maximal deImportApplicationUsage Demandes toutes les secondes par compte
Taille maximale du fichier de données d'utilisation	10 Mo	Taille maximale d'un fichier de données d'utilisation horaire.

Points de terminaison de service

Application Cost Profiler est un service global. Tous les appels d'API doivent être effectués vers le point de terminaison USA Est (Virginie du Nord).

- US East (N. Virginia) – `application-cost-profiler.us-east-1.amazonaws.com`

Sécurité dansAWSApplication Cost Profiler

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

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

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour de plus informations sur les programmes de conformité qui s'appliquent à Application Cost Profiler, veuillez consulterServices AWS concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous utilisezAWSApplication Cost Profiler Elle montre comment configurer Application Cost Profiler pour atteindre vos objectifs en matière de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autresAWSServices qui vous aident à surveiller et sécuriser vos ressources Application Cost Profiler.

Table des matières

Protection des données dans AWS Application Cost Profiler

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans AWS Application Cost Profiler. 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 plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

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) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- 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 FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

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 Application Cost Profiler ou un autre outil Services AWS à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que

vous entrez 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 un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Chiffrement au repos

AWS Application Cost Profiler chiffre toujours toutes les données stockées dans le service au repos sans nécessiter de configuration supplémentaire. Ce chiffrement est automatique lorsque vous utilisez Application Cost Profiler.

Pour les compartiments Amazon S3 que vous fournissez, vous devez chiffrer le compartiment de rapports, et vous pouvez chiffrer le compartiment de données d'utilisation et autoriser l'accès à Application Cost Profiler. Pour de plus amples informations, veuillez consulter Configuration des compartiments Amazon S3 pour Application Cost Profiler.

Chiffrement en transit

AWS Application Cost Profiler utilise Transport Layer Security (TLS) et le chiffrement côté client pour le chiffrement en transit. La communication avec Application Cost Profiler est toujours effectuée de HTTPS manière à ce que vos données soient toujours cryptées pendant le transport. Ce chiffrement est configuré par défaut lorsque vous utilisez Application Cost Profiler.

Gestion des identités et des accès pour AWS Application Cost Profiler

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. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de l'Application Cost Profiler. IAMest un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment fonctionne AWS Application Cost Profiler avec IAM

- AWS Exemples de politiques basées sur l'identité d'Application Cost Profiler
- Résolution des problèmes AWS d'identité et d'accès à Application Cost Profiler

Public ciblé

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

Utilisateur du service : si vous utilisez le service Application Cost Profiler 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 d'Application Cost Profiler 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 pouvez pas accéder à une fonctionnalité dans Application Cost Profiler, consultezRésolution des problèmes AWS d'identité et d'accès à Application Cost Profiler.

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

IAMadministrateur — Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Application Cost Profiler. Pour consulter des exemples de politiques basées sur l'identité d'Application Cost Profiler que vous pouvez utiliser dansIAM, consultez. AWS Exemples de politiques basées sur l'identité d'Application Cost Profiler

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 que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

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

(IAMIdentity 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 en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. 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 version 4 de AWS Signature pour les API demandes dans le guide de IAM l'utilisateur.

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, voir Authentification multifactorielle dans le guide de l'AWS IAM Identity Center utilisateur et Authentification AWS multifactorielle IAM dans le guide de l'IAMutilisateur.

Compte AWS utilisateur root

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 nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur 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 IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. 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 nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

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 la section Cas d'utilisation pour IAM les utilisateurs dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Pour assumer temporairement un IAM rôle dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un IAM rôle (console). Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Méthodes pour assumer un rôle dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- 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 plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur

authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à 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 connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.
- 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, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle 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. FASutilise les autorisations du principal appelant an Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes 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 les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations Service AWS dans le Guide de IAM l'utilisateur.
  - 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 IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance

et qui AWS CLI soumettent des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour 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 exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

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 JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques 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 autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

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

Politiques basées sur l’identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles

ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, voir Définir des IAM autorisations personnalisées avec des politiques gérées par le client dans le Guide de l'IAMutilisateur.

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 savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre les politiques gérées et les politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. 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 de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste 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.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d’autorisations pour une entité. Les autorisations en résultant 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 annule l’autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.
- Politiques de contrôle des services (SCPs) : SCPs JSON politiques 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 fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant 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 annule l’autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s’appliquent à la requête, les autorisations en résultant 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 IAM l'utilisateur.

Comment fonctionne AWS Application Cost Profiler avec IAM

Avant de gérer l'IAMaccès à Application Cost Profiler, vous devez connaître les IAM fonctionnalités disponibles avec Application Cost Profiler. Pour obtenir une vue d'ensemble du fonctionnement d'Application Cost Profiler et AWS des autres servicesIAM, consultez la section AWS Services qui fonctionnent avec IAM dans le guide de l'IAMutilisateur.

Rubriques

- Politiques basées sur l'identité d'Application Cost Profiler
- Politiques basées sur les ressources de l'Application Cost Profiler
- Autorisation basée sur les balises Application Cost Profiler
- Rôles du profileur IAM des coûts d'application

Politiques basées sur l'identité d'Application Cost Profiler

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées en plus des conditions dans lesquelles les actions sont autorisées ou refusées. Application Cost Profiler prend en charge des actions spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une JSON politique, consultez la section Référence des éléments de IAM JSON stratégie dans le guide de IAM l'utilisateur.

Actions

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

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

Les actions de politique dans Application Cost Profiler utilisent le préfixe suivant avant l'action : `application-cost-profiler:` Par exemple, pour autoriser quelqu'un à consulter les détails de la définition de votre rapport Application Cost Profiler, vous devez inclure l'`application-cost-profiler:GetReportDefinition`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Application Cost Profiler définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

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

```
"Action": [
      "application-cost-profiler:ListReportDefinitions",
      "application-cost-profiler:GetReportDefinition"
```

Les actions disponibles dans Application Cost Profiler sont les suivantes. Chacun autorise l'APIaction du même nom. Pour plus d'informations sur le profileur de coûts d'applicationAPI, consultez la section Référence du profileur API de coûts AWS d'application.

- `application-cost-profiler:ListReportDefinitions`— Permet de répertorier la définition du rapport pour votre AWS compte, le cas échéant.
- `application-cost-profiler:GetReportDefinition`— Permet d'obtenir les détails de la définition du rapport pour votre rapport Application Cost Profiler.
- `application-cost-profiler:PutReportDefinition`— Permet de créer une nouvelle définition de rapport.
- `application-cost-profiler:UpdateReportDefinition`— Permet de mettre à jour la définition d'un rapport.
- `application-cost-profiler:DeleteReportDefinition`— Permet de supprimer un rapport (uniquement disponible via l'Application Cost ProfilerAPI).
- `application-cost-profiler:ImportApplicationUsage`— Permet de demander à Application Cost Profiler d'importer des données d'utilisation depuis un compartiment Amazon S3 spécifié.

Ressources

Application Cost Profiler ne prend pas en charge la spécification des ressources Amazon Resource Names (ARNs) dans une politique.

Clés de condition

Application Cost Profiler ne fournit aucune clé de condition spécifique au service, mais il prend en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir Clés contextuelles de condition AWS globale dans le guide de IAM l'utilisateur.

Exemples

Pour consulter des exemples de politiques basées sur l'identité d'Application Cost Profiler, consultez. AWS Exemples de politiques basées sur l'identité d'Application Cost Profiler

Politiques basées sur les ressources de l'Application Cost Profiler

Application Cost Profiler ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises Application Cost Profiler

Application Cost Profiler ne prend pas en charge le balisage des ressources ni le contrôle de l'accès en fonction des balises.

Rôles du profileur IAM des coûts d'application

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

Utilisation d'informations d'identification temporaires avec Application Cost Profiler

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

Application Cost Profiler prend en charge l'utilisation d'informations d'identification 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 au service apparaissent dans votre IAM

compte et appartiennent au service. Un administrateur peut consulter, mais ne peut pas modifier les autorisations concernant les rôles liés à un service.

Application Cost Profiler ne prend pas en charge 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 rôles de service apparaissent dans votre IAM compte et sont détenus par le compte. Cela signifie qu'un administrateur peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Application Cost Profiler ne prend pas en charge les rôles de service.

AWS Exemples de politiques basées sur l'identité d'Application Cost Profiler

Par défaut, IAM les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources de AWS l'Application Cost Profiler. Ils ne peuvent pas non plus effectuer de tâches à l'aide du AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Un administrateur doit créer des IAM politiques qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer les API opérations spécifiques dont ils ont besoin. L'administrateur doit ensuite associer ces politiques aux IAM utilisateurs ou aux groupes qui ont besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, voir Création de politiques dans l'JSONonglet du guide de l'IAMutilisateur.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Application Cost Profiler
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accès à un compartiment Amazon S3

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Application Cost Profiler 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 plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une 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 IAM pour appliquer des autorisations, consultez la section Politiques et autorisations du Guide de IAM l'utilisateur. IAM
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. 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, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Valider les politiques avec IAM Access Analyzer dans le guide de l'IAMutilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section APIAccès sécurisé avec MFA dans le guide de IAM l'utilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console Application Cost Profiler

Pour accéder à la console AWS Application Cost Profiler, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails relatifs aux ressources Application Cost Profiler de votre AWS compte. 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 (IAMutilisateurs ou rôles) dotées de cette politique.

Pour garantir que ces entités peuvent utiliser la console Application Cost Profiler pour consulter la définition du rapport Application Cost Profiler pour votre AWS compte, attachez les autorisations suivantes aux entités.

```
application-cost-profiler:ListReportDefinitions
application-cost-profiler:GetReportDefinition
```

Par exemple, vous pouvez créer la politique suivante pour vos utilisateurs en lecture seule.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "application-cost-profiler:ListReportDefinitions",
            "application-cost-profiler:GetReportDefinition"
         ],
         "Resource":"*"
      }
   ]
}
```

Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le guide de IAM l'utilisateur.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui passent des appels uniquement vers le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'APIopération que vous essayez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accès à un compartiment Amazon S3

Dans cet exemple, vous souhaitez accorder à un IAM utilisateur de votre AWS compte l'accès à l'un de vos compartiments Amazon S3. `examplebucket` Vous souhaitez également autoriser l'utilisateur à ajouter, mettre à jour et supprimer des objets.

En plus de l'octroi des autorisations `s3:PutObject`, `s3:GetObject` et `s3:DeleteObject` à l'utilisateur, la stratégie octroie aussi les autorisations `s3:ListAllMyBuckets`, `s3:GetBucketLocation` et `s3:ListBucket`. Ces conditions supplémentaires sont requises par la console. De la même manière, les actions `s3:PutObjectAcl` et `s3:GetObjectAcl` sont nécessaires pour que les objets puissent être copiés, coupés et collés dans la console. Pour afficher un exemple de procédure détaillée permettant d'octroyer des autorisations aux utilisateurs et de les tester en utilisant la console, consultez Exemple de procédure détaillée : Utilisation de stratégies utilisateur pour contrôler l'accès à votre compartiment.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
```

```
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

Résolution des problèmes AWS d'identité et d'accès à Application Cost Profiler

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation d' AWS Application Cost Profiler et AWS Identity and Access Management (IAM).

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Application Cost Profiler
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder aux ressources de mon application Cost Profiler

Je ne suis pas autorisé à effectuer une action dans Application Cost Profiler

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 vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'`mateojackson`IAMutilisateur essaie d'utiliser la console pour afficher les détails du rapport Application Cost Profiler sans y être `application-cost-profiler:ListReportDefinitions` autorisé.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 application-cost-profiler:ListReportDefinitions on resource: Report Definition
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource de définition du rapport à l'aide de l'`application-cost-profiler:ListReportDefinitions`action.

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 Application Cost Profiler.

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 IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Application Cost Profiler. 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 politiques 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 aux ressources de mon application Cost Profiler

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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Application Cost Profiler prend en charge ces fonctionnalités, consultezComment fonctionne AWS Application Cost Profiler avec IAM.
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.

- 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 IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Validation de conformité pour AWS Application Cost Profiler

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. 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 plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne Services AWS sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- 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.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et reprennent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- 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— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dansAWSApplication Cost Profiler

L'infrastructure mondiale d'AWS repose sur les régions et les zones de disponibilité AWS. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. 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 plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour en savoir plus sur les régions AWS et zones de disponibilité , consultez Infrastructure mondiale AWS.

Sécurité de l'infrastructure dans AWS Application Cost Profiler

En tant que service géré, AWS Application Cost Profiler 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 les API appels AWS publiés pour accéder à Application Cost Profiler via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE 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 identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d’identification de sécurité temporaires et signer les demandes.

Application CoCOCOCOCOCOCOCOCOCO EventBridge

Vous pouvez utiliser Amazon EventBridge pour automatiserAWSet répondez automatiquement à des événements système tels que des problèmes de disponibilité d'application ou des modifications de ressource. Événements provenant deAWSles services sont fournis à EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour de plus amples informations, veuillez consulterAmazon EventBridge Guide de l'utilisateur.

Vous pouvez surveillerAWSApplication CoCOCOCOCOCOCOCOCO EventBridge. EventBridge achemine les données vers des cibles telles queAWS Lambdaet Amazon Simple Notification Service (Amazon SNS). Ces événements sont les mêmes que ceux qui apparaissent sur Amazon CloudWatch Events, qui offre une near-real-time flux d'événements système qui décrivent les modifications apportéesAWSAWS.

Surveillez la génération de rapports avec EventBridge

avec EventBridge, vous pouvez créer des règles définissant les actions à mettre en œuvre lorsque Par exemple, vous pouvez créer une règle qui vous envoie un e-mail chaque fois qu'un rapport est généré.

Pour surveiller la génération de rapports

1. Connectez-vous àAWSà l'aide d'un compte autorisé à utiliser à la fois EventBridge Application CoCOCOCOCOCOCOCOCO
2. Ouvrez l'Amazon EventBridge Consolehttps://console.aws.amazon.com/events/.
3. À l'aide des valeurs suivantes, créez un EventBridge règle qui surveille les événements créés lors de la génération d'un rapport :

   - Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
   - PourOrigine de l'événement, choisissezAutre.
   - DansModèle d'événementsection, choisissezModèle personnalisé (éditeur JSON), puis collez le modèle d'événement suivant dans la zone de texte :

```
{
  "source": ["aws.application-cost-profiler"],
```

```
  "detail-type": ["Application Cost Profiler Report Generated"]
}
```

- PourTarget, choisissezAWSservice, et pourSélectionnez une cible, choisissez leAWSle service que vous voulez EventBridge détecte un événement du type sélectionné. La cible est déclenchée lorsqu'un événement correspond au modèle d'événement défini dans la règle est reçu.

Pour obtenir des informations sur la création de règles, consultezCréation d'Amazon EventBridge règles qui réagissent aux événementsdans leAmazon EventBridge Guide de l'utilisateur.

Exemple d'événement généré par un rapport

Cet événement vous informe lorsqu'un rapport est généré et prêt à être récupéré. Le`message`vous fournit le compartiment Amazon Simple Storage Service (Amazon S3) et la clé pour l'objet Amazon S3 dans lequel le rapport est stocké.

```
{
   "version": "0",
   "id": "01234567-EXAMPLE",
   "detail-type": "Application Cost Profiler Report Generated",
   "source": "aws.application-cost-profiler",
   "account": "123456789012",
   "time": "2021-03-31T10:23:43Z",
   "region": "us-east-1",
   "resources": [],
   "detail": {
     "message": "Application Cost Profiler report delivered in bucket: SampleBucket,
 key: SampleReport-112233445566"
   }
}
```

Historique du document

Le tableau suivant décrit les versions de documentation pourAWSProfileur des coûts d'application.

Modification	Description	Date
Notification de désapprobation du service	AWSApplication Cost Profiler ne sera plus disponible d'ici le 30 septembre 2024 et n'accepte plus de nouveaux clients.	11 août 2023
Surveillance des événements	En raison des modificat ions apportées auEventBr idgeconsole, la façon dont vous créez des règles pour surveiller les événements d'Application Cost Profiler a changé. Pour plus d'informa tions, voirSurveillance des événements du profileur des coûts d'application dansEvent Bridge.	5 juillet 2022
Mises à jour d'exemples de politiques relatives aux compartiments S3	Mise à jour uniquement documentaire des exemples de politique de compartim ent S3. Pour plus d'informa tions, voirConfiguration des compartiments Amazon S3 pour Application Cost Profiler.	6 décembre 2021
Disponibilité générale	La première version publique d'Application Cost Profiler.	13 mai 2021